PRIVACY IN THE COMMERCIAL WORLD II

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JUNE 20, 2006

Serial No. 109-99

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

29-729PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

CLIFF STEARNS, Florida, *Chairman*

FRED UPTON, Michigan
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
JOE BARTON, Texas
(EX OFFICIO)

JAN SCHAKOWSKY, Illinois
Ranking Member
MIKE ROSS, Arkansas
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
SHERROD BROWN, Ohio
BOBBY L. RUSH, Illinois
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
JIM DAVIS, Florida
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
JOHN D. DINGELL, Michigan
(EX OFFICIO)

CONTENTS

PRIVACY IN THE COMMERCIAL WORLD II

TUESDAY, JUNE 20, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON COMMERCE, TRADE,
AND CONSUMER PROTECTION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:40 p.m., in Room 2123, Rayburn House Office Building, Hon. Cliff Stearns [chairman] presiding.

Present: Representatives Stearns, Deal, Radanovich, Terry, Otter, Blackburn, Barton [ex officio], Schakowsky, and Gonzalez.

Staff Present, David Cavicke, General Counsel; Shannon Jacquot, Counsel; Chris Leahy, Policy Coordinator; Brian McCullough, Professional Staff Member; Will Carty, Professional Staff Member; Billy Harvard, Legislative Clerk; Kelly Cole, Counsel; Consuela Washington, Minority Senior Counsel; Alex Gerlach, Minority Research Assistant; and Jonathan Brater, Minority Staff Assistant.

MR. STEARNS. Good afternoon. The subcommittee will come to order. The Commerce, Trade, and Consumer Protection Subcommittee first began to work on comprehensive consumer privacy issues back in 2001 when we had a series of hearings on all facets of this issue, including commercial privacy policy, government privacy practices, and related consumer protection issues.

In fact, our first hearing, aptly titled "Privacy in the Commercial World," was held over 5 years ago. Today's installment of that series, part II, has been a long time in coming, but the time is right to revisit comprehensive privacy after spending over 5 years on several of its elements, including legislative work on spyware, pretexting, and, most recently, data security legislation, which, it is my hope, will be brought to the floor for a vote very soon.

My colleagues, the 5 years since the first privacy hearing back in 2001 also has been a period marked by the September 11 attacks, which not only unleashed the military might of the United States, but also its ingenuity in using advanced technology, information collection, and sophisticated analyses as one of the major weapons countering the forces of terrorism and totalitarianism around the world.

While certain things have changed since the first hearing, a great deal remains the same. The United States continues to regulate privacy under a sector-specific disjointed approach, managing an ever-increasing number of local, State and Federal requirements dealing with notice, consent, and security protections in the health, on-line financial, and other contexts. Although this collection of laws has increased, our protection against privacy-infringing practices, and, to a lesser degree, identity theft, this body of law still contains gaping holes and major inconsistencies that leave consumers unprotected and businesses with uncertainties that directly affect their success.

My hope, when I first introduced my bill, H.R. 1263, the Consumer Privacy Act of 2005, was to start the process of developing a consistent, Federal approach to privacy. Back then, the committee was focused on constructing an approach to privacy that could become an overlay on all the work that has been done in the area of commercial privacy. The approach would offer better uniformity and more efficient regulation as information technology, as the use of consumer information, and domestic and international commerce continued to become more integrated and in some cases converge. More uniform, stronger, and more consistent consumer protection was and still remains our goal. Accordingly, the committee today would like to reenergize this effort with those principles and objectives in mind. The subcommittee plans to continue its long-term examination of privacy issues with additional hearings and will begin to work through a draft bill.

As I have said, a fundamental principle and one of the main drivers of our efforts in the area of privacy is to establish a uniform and consistent privacy regime for the American consumers and for American businesses. In addition, we need to empower consumers, businesses, and the Federal government to make the application and enforcement of privacy practice in the United States the world benchmark. With regard to data protection, we will examine how our work and data security can complement and enhance a national privacy regime. Further, I believe the Congress needs to take a closer look at international regulation of privacy, both how the national and supranational level is affecting U.S. business and its ability to compete globally. We continue to be concerned about the privacy practices of other countries compromising the business decisions of some of our most successful and innovative companies.

The outcome we are seeking from our efforts in this area is the assurance that the consumer has the knowledge and the control to make informed decisions that involve personal information, and that businesses have a consistent framework of law and regulation that stimulate innovation and success rather than hampering those goals. New

technology continues to allow better and more efficient decisions and transactions in the commercial world. We need to encourage that innovation because it is what enables our businesses in the United States to lead the rest of the world. That is a leadership edge that we cannot compromise. We do, however, need to recognize that as information technology and information sharing become more powerful, the ability to harm becomes just as powerful, and, as we have seen, ultimately destructive. Identity theft remains a top concern for this committee and the American consumer. Therefore, rigorous data security and data security policies are essential if we are to protect the progress that we are making in this area.

In closing, the subcommittee has established, without question, the most comprehensive record on privacy and information security issues in our Congress. This is a foundation that was built over years of studying these issues and working through some very good ideas and a number of legislative proposals. It is time to continue that important task. To reinitiate our work in the privacy area, I am particularly happy to have several leaders in commercial privacy, from business and from academia before us today, including Ms. Meg Whitman, President and CEO of eBay. I want to thank all of you for joining us and offering your views today. I look forward to continuing this important work and engaging all stakeholders, consumer groups, businesses, government, and academia, to craft sound, proactive, and necessary legislation in the field of consumer privacy that will spur innovation, protect consumers, and ensure that all American businesses will continue to lead the world with its innovation, productivity, and with regard for the privacy of the consumers that it serves.

With that, Ms. Schakowsky is recognized.

[The prepared statement of the Hon. Cliff Stearns follows:]

PREPARED STATEMENT OF THE HON. CLIFF STEARNS, CHAIRMAN, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

Good afternoon. The Commerce, Trade and Consumer Protection Subcommittee first began to work on comprehensive consumer privacy issues back in 2001, when we had a series of hearings on all facets of the issue, including commercial privacy policy, government privacy practices, and related consumer protection issues. In fact, our first hearing, aptly titled "Privacy in the Commercial World" was held over five years ago. Today's installment of that series, "Part Two", has been a long time in coming, but the time is right to revisit comprehensive privacy after spending over five years on several its elements, including legislative work on spyware, pre-texting, and, most recently, data security legislation, which I hope will be brought up for a House vote soon. The five years since that first privacy hearing back in 2001 also has been a period marked by the September 11th attacks, which not only unleashed the military might of the United States but also its ingenuity in using advanced technology, information collection, and sophisticated analysis as one of the major weapons countering the forces of terrorism and

totalitarianism around the world. And while certain things have changed since that first hearing, a great deal remains the same. The United States continues to regulate privacy under a sector-specific, disjointed approach -- managing an ever-increasing number of local, state, and federal requirements dealing with notice, consent, and security protections in the health, on-line, financial, and other contexts. Although this collection of laws has increased our protections against privacy-infringing practices and to a lesser degree identity theft, this body of law still contains gaping holes and major inconsistencies that leave consumers unprotected and business with uncertainties that directly affect their success.

My hope when I first introduced my bill, HR 1263, the "Consumer Privacy Act of 2005" was to start the process of developing a consistent, federal approach to privacy. Back then, the Committee was focused on constructing an approach to privacy that could become an overlay on all the work that has been done in the area of commercial privacy. The approach would offer better uniformity and more efficient regulation as information technology, the use of consumer information, and domestic and international commerce continue to become more integrated, and in some cases, converge. More uniform, stronger, and more consistent consumer protection was and still remains the goal. Accordingly, the Committee today would like to re-energize this effort with those principles and objectives in mind. The Subcommittee plans to continue its long-term examination of privacy issues with additional hearings, and will begin to work through a draft bill.

As I have said, a fundamental principle and one of the main drivers of our efforts in the area of privacy is to establish a uniform and consistent privacy regime for the American consumer and business. In addition, we need to empower consumers, business, and the federal government to make the application and enforcement of privacy practices in the United States the world benchmark. With regard to data protection, we will examine how our work in data security can complement and enhance a national privacy regime. Further, I believe the Congress needs to take a closer look at how international regulation of privacy, both and the national and supranational level, is affecting U.S. business and its ability to compete globally. We continue to be concerned about the privacy practices of other countries compromising the business decisions of our some of our most successful and innovative companies.

The outcome we are seeking from our efforts in this area is the assurance that the consumer has the knowledge and the control to make informed decisions that involve personal information, and that business has a consistent framework of law and regulation that stimulates innovation and success, rather than hampering those goals. New technologies continue to allow better, more efficient decisions and transactions in the commercial world. We need to encourage that innovation because it is what enables U.S. business to lead the rest of the world. That is a leadership edge that we cannot compromise. We do, however, need to recognize that as information technology and information sharing become more powerful the ability to harm becomes just as powerful and, as we have seen, destructive. Identity theft remains a top concern for this Committee and American consumers. Therefore, rigorous data security and data security policies are essential if we are to protect the progress that we are making in this area.

In closing, this Subcommittee has established, without question, the most comprehensive record on privacy and information security issues in the Congress. This is a foundation that has been built over years of studying these issues and working through some very good ideas in a number of legislative proposals. It is time to continue that important task. To reinitiate our work in the privacy area, I am particularly happy to have several leaders in commercial privacy from business and academia before us today, including Ms. Meg Whitman, President and CEO of eBay. Thank you all for joining us and offering your views today. I look forward to continuing this important work, and engaging all stakeholders --consumer groups, business, government, and academia to

craft sound, proactive, and necessary legislation in the field of consumer privacy -- legislation that will spur innovation, protect consumers, and ensure that American business will continue to lead the world with it's innovation, productivity, and regard for the privacy of all the consumers it serves.

Thank you.

MS. SCHAKOWSKY. Thank you, Chairman Stearns, for convening today's hearing on privacy and the commercial world.

As our committee knows all too well, the transition from shopping on Main Street to e-commerce has created new and unique challenges that make current laws inadequate to protect consumers' right to privacy. I am glad that we are exploring ways to close the gaps in the law that put consumers' sensitive information at risk.

Although most industrialized nations have comprehensive privacy protection laws, the United States has had a piecemeal, fragmented approach, regulating by industry and product. Our committee is guilty of perpetuating this haphazard approach. We regulate by headline the problem of the day, be it spam, spyware, pretexting for phone records or information brokers.

To our credit, we have been trying to close loopholes, but at the same time we have pushed off the big question of establishing broad privacy principles for another day. I am glad that we are now moving forward to address this important issue.

This piecemeal approach is also perpetuated by financial, commercial, and other industries that have labeled even the minimal privacy protections we put forth as too burdensome. However, I am sure you all know the old adage that with great power comes great responsibility.

The Internet and the advances in technology have given the industry great power to reach consumers, sell their wares, and compile large databases of information. The expansion of their reach also means that industry has also a greater responsibility to protect consumers and their private, personal information.

I am pleased to hear that a number of industry leaders have come together, along with Professor Peter Swire, who has a long history of promoting consumer privacy, to start exploring broad legislation that would close the gaps in the law and set privacy principles that all industry should follow both on and off line.

Since we are just beginning these discussions, it is unclear whether we will be able to agree on a common product. Nevertheless, I am glad that some in industry are beginning to shift their thinking about personal consumer information and privacy.

However, we shouldn't limit our scope to commercial practices. We should thoroughly examine government practices as well. Although we

have one of the most secretive administrations in our country's history, it simultaneously has been the most invasive into the public's privacy.

As I mentioned before, our committee unanimously passed legislation, the Prevention of Fraudulent Access to Phone Records Act, in order to better secure private phone records and put control of personal calls back in consumers' hands.

However, that bill seems to have disappeared to an unclosed location. Eight days after it was pulled from the floor schedule, USA Today broke the story that the National Security Agency was acquiring the public's phone records from three of the major carriers, without subpoenas, warrants, or any approval from the courts.

If true, it has occurred without consumers' knowledge or consent and with total disregard to the Privacy Act and other laws like FISA, the Foreign Intelligence Surveillance Act, that govern how our intelligence agencies operate.

Chairman Stearns, as you may recall, I along with every Democrat on our committee sent a letter to Chairman Barton calling for a hearing on the allegations concerning the phone companies and the NSA. That letter was sent on May 11, and we still have not received a response. If we are serious about privacy, about closing the loopholes, getting beyond patchwork legislation, then we cannot turn a blind eye to what is happening in our own backyard and the total disregard for privacy laws on the books by the Administration. We are urging a response very soon. We would appreciate your help. This issue is not going away.

Additionally, I think we need to look into the strong-armed tactics the Administration is employing to stopping investigations into its antiprivacy practices. New Jersey and other States have been exploring whether the phone companies sharing of records is in violation of their privacy laws. In retaliation, on June 15, the Justice Department brought a suit against the New Jersey Attorney General Zulima Farber, to stop him from seeking information about the telephone companies cooperation with the NSA. The rolling out of the disclaimer that it is in the interest of national security does not give the Administration a free pass to trample on civil liberties and States' rights and sue those who are trying to protect the American public from privacy invasions.

Again, I look forward to hearing from today's witnesses, and I thank you.

MR. STEARNS. The gentlewoman from Tennessee, Mrs. Blackburn, is recognized.

MRS. BLACKBURN. Thank you, Mr. Chairman. I want to thank you for your commitment to this issue and for holding the hearing today and for looking at different ways for Congress to act to protect privacy, the right to privacy, the expectation of privacy, and the expectation of

security. That is something that our constituents are interested in, and they are interested to see how we are going to be certain that we respect their right to privacy and at the same time meet their concerns on how we remain a secure Nation.

My constituents in my district have expressed their concerns on identity theft to me. We have had some town halls on identity theft, specifically on this issue. I think that the data bill that passed out of committee is a good solid first step on addressing that problem. I am looking forward to continuing on that and working on that issue, but we still need to address the privacy protections regarding the buying and selling of consumer information.

I know many people have stated that the EU has much better privacy protections than the U.S., and I believe the FTC should study the European Union's standards and see if we should incorporate some of them, any of them, or a part of that into our regulations.

Another concern that I have is that there have been several instances of foreign companies obtaining financial information of Americans and using this information to conduct identity theft. When we hear of this, it is of tremendous concern, and I hope it is of concern to each one of the guests who are with us today.

This will almost certainly continue until either two things happen, either one or the other: either the Federal government will oversee international transactions of consumer data, or an outright prohibition of these transactions is implemented. I am not one to want to hinder global commerce, but if it is required to protect the private information of American citizens, then maybe that is something we need to put on the table and talk about.

One other area that needs to be addressed is the relative ease of being able to sell consumer information. I believe that one possible way to protect this data is to ensure businesses do a preliminary background information of the buyers of the information.

Mr. Chairman, these are just a few of the concerns. I look forward to the hearing, and I yield the balance of my time.

MR. STEARNS. I thank the gentlewoman. The gentleman from Texas, Mr. Gonzalez.

MR. GONZALEZ. I waive opening. Thank you.

MR. STEARNS. The gentleman waives opening.

The Chairman of the Full Committee, the gentleman from Texas, Mr. Barton.

CHAIRMAN BARTON. Thank you, Mr. Chairman. Good afternoon to our witnesses. I want to thank you, Chairman Stearns, for holding this hearing and Congresswoman Schakowsky, the Ranking Member, for being supportive of the hearing.

I am a co-chair of the Congressional Privacy Caucus. I think that protecting the privacy of our citizens is one of the most important things that we have an obligation to do, and I think it is time for Congress to begin to honor that obligation.

It seems like if not every week, every month now we get some widely publicized data security breach, and they seem to be getting worse instead of better. Last week we held a hearing, the Oversight and Investigations Subcommittee, where we found out that the agency within the Department of Energy, which is responsible for security of our nuclear secrets was, itself, breached and over 1,500 records stolen of the personnel of that agency, along with their Social Security number. That is at an agency that is tasked with protecting the secrets of our nuclear weapons program.

It is no surprise, then, that the public has become increasingly alarmed by the prevalence of crimes of data security breaches and how their personal information is more and more able to be shared in the commercial world. Citizens are looking both to the entities which have their information and to the Congress to take action to correct this problem.

To that end, this committee and this subcommittee introduced the Data Act. Through bipartisan work, the committee passed that act 42-0. It is waiting to go to the floor, and has been hung up from going to the floor of the House of Representatives because another committee with no jurisdiction feels threatened and the industry that has issues before that committee feels threatened. So that bill that passed 42-0 has not yet been scheduled for a floor vote in this Congress.

It is my intention to encourage the leadership to bring that bill to the floor as soon as possible, and I have had meetings about that and discussions about that today.

This subcommittee has also held a hearing on the issue of Social Security numbers in commerce and how best to balance beneficial uses with the threats to personal privacy.

However, these two issues are only a few of the many pieces of the privacy puzzle, and I think it is time to stop doing things on a piecemeal basis and to introduce comprehensive legislation. That is the purpose of this hearing today, to see if there is support for a comprehensive approach to privacy protection.

It is my belief that individuals must be informed in a clear and conspicuous manner when private companies or government agencies plan to collect, use, or disclose personally identifiable information. Let me repeat that. It is my belief that the citizens of the United States of America must be informed in a clear and conspicuous fashion when

private companies or governmental agencies are going to collect, use, or disclose personally identifiable information.

I believe that consumers must be told with whom any information is going to be shared and why. For the most sensitive information, an opt-in should be the standard operating procedure. This information should not be shared at all unless an individual gives his or her express consent.

Congress has dealt with the issue of consumer privacy protection, if at all, in the past on a sector-by-sector basis.

As I said earlier, it is my belief that it is time now for a broader, more comprehensive approach. Issue-specific, stop-gap measures are no longer enough. I think it is ludicrous to claim that Gramm-Leach-Bliley is privacy protection. It is disclosure. It is not, in my opinion, privacy protection.

Consumers' privacy is at risk in too many areas that are not covered. An increasingly complex patchwork of State and Federal laws has not been effective in serving the interests of consumers, and, at the same time, it has required businesses to navigate sometimes inconsistent legal obligations.

Furthermore, growing anxiety about consumers and identity theft has begun to erode public trust and the safety of their information. It is inevitable that this will threaten on-line commerce, the Internet, and commerce in general if this situation is not corrected.

Last year, I was very glad to see a coalition of high-technology companies come together with the goal of working towards some widely agreed-upon principles for privacy legislation.

As I understand it, their stated goals are twofold: to establish a strong baseline privacy protection for consumers; and to provide organizations with a uniform standard on which they can build effective privacy policies and compliance efforts. I think this is a great starting point, and I absolutely applaud their efforts.

I am glad that we have some members of that coalition here today, and I am anxious to hear more of the progress of their work. These are complex issues, and there is considerable repercussion among consumers in the industry if we move in this area.

However, I think the repercussions are larger if we don't move. If we fail to act, organizations will face increasing costs associated with consistent and overlapping obligations. Consumers will feel even more tentative and even more worried about disclosing personal information.

Without action, the vitality of e-commerce and the potential of the Internet as a significant economic force will be in jeopardy. I am glad to work with the private sector as we discuss how to implement the appropriate consumer protections, while giving businesses a set of the

Federal rules of the road that provide certainty without requiring an overly burdensome compliance regime.

I wish to thank my co-chairman of the Privacy Caucus, Mr. Edward Markey of Massachusetts, for his work in this area. He and others on both sides of the aisle are going to work very aggressively to put together a draft bill and hopefully mark it up and bring it to the floor of the House in this Congress. Not in the next Congress, in this Congress.

Thank you again, Mr. Chairman, and Ranking Member Schakowsky, for hosting this hearing. I yield back the balance of my time.

[The prepared statement of the Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Good afternoon. Thank you, Chairman Stearns, for holding this hearing. This is an issue that is very important to me, and as co-chair of the Congressional Privacy Caucus, I plan to work toward putting together comprehensive privacy legislation to be considered in this Congress.

The widely-publicized data security breaches of the last year and a half have coincided with the public's increased awareness of the relationship between identity theft and their personal information. Not surprisingly, the public has become increasingly alarmed by the prevalence of this crime and by how their personal information is shared in the commercial world. Many citizens are looking both to the entities which have their information and to Congress to take action to correct this problem. To that end, this committee introduced the DATA Act, and through bipartisan work, the Committee agreed unanimously to provide strong protections and remedies for American consumers and the security of their personal information. It is my intention to bring that bill to the House floor for a vote. This subcommittee also recently held an important hearing on the uses of Social Security numbers in commerce, and how best to balance beneficial uses with the threats to personal privacy. However, these are only a couple of pieces of the privacy puzzle, and I believe further legislation is needed.

Individuals must be informed in a clear and conspicuous manner when private companies or governmental agencies plan to collect, use, or disclose personally identifiable information. I believe that consumers must be told with whom any information may be shared and why. For the most sensitive information, an "opt-in" should be the standard. This information should not be shared at all unless one gives his or her express consent.

Historically, Congress has dealt with the issue of consumer privacy sector by sector, but it is time for a broader, more comprehensive approach. Issue-specific, stop-gap measures are no longer enough. Consumers' privacy is at risk in too many areas that are not covered. An increasingly complex patchwork of state and federal laws has not been effective in serving the interest of consumers, and at the same time, it has required businesses to navigate sometimes inconsistent legal obligations. Furthermore, growing anxiety among consumers about privacy and ID theft has begun to erode public trust in the safety of their information. It is inevitable that this will threaten online commerce, the Internet, and commerce in general if the situation is not corrected.

Late last year, I was very glad to see a coalition of high-tech companies come together with the goal of working toward some widely agreed upon principles for privacy legislation. As I understand it, their stated goals are twofold: to establish strong baseline privacy protections for consumers, and to provide organizations with a uniform standard on which they can build effective privacy policies and compliance efforts. I think this is

a great starting point, and I absolutely applaud their efforts. I am glad we have some members of that coalition here today, and I am anxious to hear more about the progress of their work.

Obviously, these are complex issues with considerable repercussions for consumers and for industry. If we fail to act however, organizations will face increasing costs associated with inconsistent and overlapping obligations, and consumers will feel even more tentative and more worried about disclosing personal information. Finally, without action, the vitality of e-commerce and the potential of the Internet as a significant economic force may be in jeopardy. I am glad to work with the private sector as we discuss how we can implement the appropriate consumer protections, while giving businesses a set of federal "rules of the road" that provide certainty without requiring an overly burdensome compliance regime.

I want to thank all our expert witnesses for participating today, and I look forward to working with all stakeholders to put together essential and historic privacy legislation.

Thank you, and I yield back the balance of my time.

MR. STEARNS. I thank the gentleman.

MR. STEARNS. Mr. Terry.

MR. TERRY. I have no statement.

MR. STEARNS. With that, we will move to the opening--do you waive, Mr. Terry?

MR. TERRY. Yes, I waive.

MR. STEARNS. All right, then you will have additional time.

We are very pleased to move to our panel. Ms. Meg Whitman is President and CEO of eBay; Dr. Thomas M. Lenard, Ph.D., Senior Vice President for Research, The Progress & Freedom Foundation; Professor Peter Swire, C. William O'Neill Professor of Law at Ohio State; Mr. Scott Taylor, Chief Privacy Officer for Hewlett-Packard Company; and Mr. Evan Hendricks, Editor/Publisher of Privacy Times.

STATEMENTS OF MEG WHITMAN, PRESIDENT AND CEO, eBAY INC.; THOMAS M. LENARD, Ph.D., SENIOR VICE PRESIDENT FOR RESEARCH, THE PROGRESS & FREEDOM FOUNDATION; PETER SWIRE, C. WILLIAM O'NEILL PROFESSOR OF LAW, MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY; SCOTT TAYLOR, CHIEF PRIVACY OFFICER, HEWLETT-PACKARD COMPANY; AND EVAN HENDRICKS, EDITOR/PUBLISHER, PRIVACY TIMES

MR. STEARNS. Ms. Whitman, welcome, and we appreciate your opening statement.

MS. WHITMAN. Thank you, Chairman Stearns and members of the committee. I appreciate the chance to talk to you today about what I believe is the pressing need for Federal privacy legislation.

As Chairman Barton mentioned, my name is Meg Whitman, and I am the President and Chief Executive Officer of eBay, Inc. eBay, as most of you probably know, enables commerce on a local, national, and international basis with an array of Web sites, including eBay, PayPal, Skype, Kijiji, Rent.com, and Shopping.com. We bring together millions of buyers and sellers every day to meet, talk, and trade.

eBay's purpose, pioneering new communities around the world, built on commerce, sustained by trust, and inspired by opportunity, relies heavily on our commitment to protect our users' privacy. That is why we believe it is critical to safeguard privacy in a variety of ways.

We tell our users how we use their personal information in a transparent, concise, plain English, privacy policy that is linked from every single page of our Web site. We do not share, rent, or sell personally identifiable information to third parties for marketing purposes.

Our payment service, PayPal, provides consumers with a safe way to shop without sharing their financial information, thereby reducing the possibility of identity theft.

The eBay toolbar helps consumers detect fraudulent Web sites and the eBay Web site provides detailed information to our users about threats to their privacy and security.

In fact, eBay's commitment to privacy is so strong that consumers have recognized our efforts by naming us as one of the companies they most trust to protect their privacy.

Most importantly, we believe that these safeguards are just one component of a national privacy protection framework. With this in mind, eBay supports the efforts to enact Federal privacy legislation establishing consistent national standards.

Comprehensive and preemptive Federal privacy legislation will promote and protect individual privacy, and will help unify today's patchwork of laws, some Federal, some State, some applying to all businesses, some focused on particular business sectors, some general, some technology specific which consistently will help the millions of small businesses who sell on eBay limit the growing cost of compliance, while providing a uniform, meaningful, and understandable set of protections for consumers.

With new technologies raising new privacy issues almost every day, it is time to lay the foundation for a long-term approach to privacy protection. If I may, I would like to suggest some principles to guide the drafting of thoughtful legislation in this area.

First, Federal privacy legislation should create a strong unified national standard that would occupy the field and preempt State laws. Legislation without preemption would make the current situation

possibly worse, not better, by creating additional uncertainty and compliance burdens.

Second, in order to maintain trust and ensure the appropriate protections for consumers, Federal standards must be enforced. We at eBay are committed to employing strong privacy practices for our consumers, and I know that many of my colleagues in the tech community feel the same. But something must be done to hold the bad actors accountable for failing to put the safety and security of their consumers before other interests.

Strong enforcement by the Federal Trade Commission is critical. A private right of action would be counterproductive in this emerging area of the law, marked by rapidly evolving technology, standards, and practices.

Third, any legislation must apply broadly and not burden any single sector or technology. A law that discriminated against e-commerce, when all companies are increasingly handling growing volumes of consumers' information, would be both unfair and ineffective in covering the broad challenges to consumer privacy. Treating consumers' data differently, depending on the type of business that collects it, would likewise be problematic.

Fourth, Federal privacy legislation should accord with the sound data protection rules adopted by our country's leading international trading partners and allies, covering reasonable notice, consumer consent regarding use and disclosure of information, practical access to data, general security standards and government enforcement authority. Businesses selling internationally to consumers around the world benefit from consistent trading rules, including consistent privacy protections.

Building on these guiding principles, industry, government, and consumers must work together to protect privacy, while we and other companies continue to work to protect our users' privacy. Federal privacy legislation is the next step in a comprehensive approach to privacy protection.

Mr. Chairman, members of the committee, thank you again for inviting me to testify here today. I will be happy to answer the question when the time comes.

MR. STEARNS. Thank you.

[The prepared statement of Meg Whitman follows:]

PREPARED STATEMENT OF MEG WHITMAN, PRESIDENT AND CEO, EBAY, INC.

Thank you Chairman Barton, Chairman Stearns and members of the Committee. I appreciate the chance to talk with you today about the pressing need for federal privacy legislation.

My name is Meg Whitman and I am the President and Chief Executive Officer of eBay Inc. eBay enables ecommerce on a local, national, and international basis with an array of websites – including the eBay Marketplaces, PayPal, Skype, Kijiji, Rent.com and Shopping.com – that bring together millions of buyers and sellers every day to trade on the world's online marketplace.

eBay's purpose -- pioneering new communities around the world built on commerce, sustained by trust, and inspired by opportunity -- relies heavily upon our commitment to protect our users' privacy. That is why we believe it is critical to safeguard our users' privacy in a variety of ways:

- eBay does not share, rent or sell personally identifiable information to third parties for marketing purposes, unless users expressly opt in.
- eBay's PayPal provides consumers a safe way to "shop without sharing" their financial information, thereby reducing the possibility of identity theft.
- eBay's toolbar helps consumers detect fraudulent websites, and
- eBay's website provides detailed information to our users about threats to their privacy and security.

In fact, eBay's commitment to privacy is so strong that consumers have recognized our efforts by naming us as one of the companies they most trust to protect their privacy.

Most importantly, we believe that these safeguards are just one component of a national privacy protection framework. With this in mind, eBay supports the effort to enact federal privacy legislation establishing consistent national standards.

Comprehensive and preemptive federal privacy legislation will promote and protect individual privacy and will help unify today's crazy-quilt of laws – some federal, some state; some applying to all businesses, some focused on particular business sectors, some general, some technology-specific. Consistency will help eBay businesses limit the growing costs of compliance, while providing uniform, meaningful, and understandable protections for consumers. With new technologies raising new privacy issues, it is time to lay the foundation for a long-term approach to privacy protection.

Permit me to suggest some principles to guide the drafting of thoughtful legislation in this area:

First, federal privacy legislation should create a strong unified national standard that would "occupy the field" and preempt state laws. Legislation without preemption would make the current situation worse, not better, by creating additional uncertainty and compliance burdens.

Second, in order to maintain trust and ensure the appropriate protections for consumers, federal standards must be enforced. We at eBay are committed to employing strong privacy practices for our consumers, and I know that many of my colleagues in the tech community feel the same. But something must be done to hold the bad actors accountable for failing to put the safety and security of their consumers before other interests. Strong enforcement by the Federal Trade Commission is critical. A private right of action would be counter-productive in this emerging area of the law marked by rapidly evolving technology, standards, and practices.

Third, any legislation must apply broadly, and not burden any single sector or technology. A law that discriminated against ecommerce when all companies are increasingly handling growing volumes of consumer information would be both unfair and ineffective in covering the broad challenges to consumer privacy. Treating consumer data differently depending on the type of business that collects it would likewise be problematic.

Fourth, federal privacy legislation should accord with the sound data protection rules adopted by our leading trading partners and allies, covering reasonable notice, consumer consent regarding use and disclosure of information, practical access to data, general security standards, and government enforcement authority. Businesses selling

internationally to consumers around the world benefit from consistent trading rules, including consistent privacy protections.

Building on the guiding principles, industry, government, and consumers must work together to protect privacy. While we and other companies will continue to work to protect our users' privacy, federal privacy legislation is the next logical step in a comprehensive approach to privacy protection.

Mr. Chairman, members of the Committee, thank you again for inviting me to testify today. I'd be happy to answer any questions.

MR. STEARNS. Dr. Lenard, you could just use her microphone or the other one.

MR. HENDRICKS. Excuse me, Mr. Chairman. I have a "can't miss" train.

MR. STEARNS. If that is okay with the rest of you, we should be through here. Each of you has 5 minutes.

Mr. Hendricks.

MR. HENDRICKS. Thank you, I appreciate it. It is great to be at a hearing where so many points I don't have to make, because you have made them, Mr. Chairman, and the Ranking Member has made them, and the Chairman of the Full Committee has made some very important points. That will save us a lot of time. I appreciate that. Thanks to the members here for letting me go.

I think that I really salute your leadership on this issue and could not agree more on the need for comprehensive privacy legislation. In a sense, this is a back-to-basics, a return to fundamentals, because our privacy policy started in the early 1970s when Senator Sam Irvin introduced the Privacy Act, and he wanted one law covering both the Federal agency sector and the private sector, and he also wanted a national oversight office to enforce and implement our privacy policy. He got half a loaf.

The Privacy Act covered the Federal agencies. We settled for a study commission to study the private sector. Since then what has happened, as the Ranking Member said, we have legislated by anecdote, and we have a hodgepodge of laws. Naturally States have moved in to fill the gap where Federal law has not been able to address issues.

So as we look now at revisiting the need for a comprehensive law, I think the first thing you have to realize is to get a comprehensive law that will bring more uniformity, you have to start from a high threshold of protection. To start from a high threshold of protection, you need to return to the fundamentals, the eight leading fair information practice principles that are outlined in the guidelines in the Organization for Economic Co-operation and Development. Those were endorsed by the U.S. Government and most Western governments, Japan and many others.

If you walk through those quickly, you can see that the first principle of openness basically means access to information. I think why we have such an encouraging start here is the corporate leadership at this table is definitely leaning in favor of an access standards. That is one of the first areas that must be addressed.

Other areas that are very important are to specify uses of information and limit uses that will not be permissible. The other thing is participation means to be able to correct errors that are in records. Most of these are reflected in the Fair Credit Reporting Act, one of our first privacy laws.

Another thing that is getting a lot of ink lately is the need for security safeguards. In fact, we have security safeguard standards in both the Privacy Act of 1974 and the Gramm-Leach-Bliley Act. I couldn't agree more with the Chairman that the Gramm-Leach Bliley Act does not represent privacy protection to the extent that we need it in these days.

Collection limitation is an important principle, and two examples of it would be to limit the collection of Social Security numbers, an issue this subcommittee has wrestled with, as well as the use of encryption technology, so that we limit the collection of information or its usefulness once it is stored.

The final issue and one of the toughest issues is accountability, which means enforcement. There, I would commend the subcommittee to the model created by the Fair Credit Reporting Act, which represents the goal of democratizing enforcement. When you have 200 million people who are the subject of records, you need to spread enforcement as far and as wide as you can.

The Fair Credit Reporting Act does that by giving certain jurisdiction to other agencies, others to State Attorneys General, and finally you need to have a private right of action to continue our tradition of putting responsibility on the individual to stand up and defend his own rights.

The final thing in closing I would like to say, Mr. Chairman, is along with this, is you also need privacy infrastructure. We seek that. We have examples of that. Right here next to me is a Chief Privacy Officer. You have people, you have resources in place to implement and oversee privacy policy. Hewlett-Packard is one early establisher of one of these offices. Many fine companies have done that.

Congress has mandated this by the Department of Homeland Security by having a statutorily mandated chief privacy officer, as are more and more of the Federal agencies.

What we don't have, what every other country has, is a national privacy office. Peter Swire could probably explain a little more about this, because he had some of that role when he was in the past administration. But other countries I have seen have gotten great

mileage and great returns for rather minimal investment from having a national privacy office that can oversee policy, provide guidance to government agencies, handle complaints and be a resource for the legislative branch and the media and the public.

That is what I see as some of the outlines of the comprehensive policy. I will work extra hard to answer this committee's questions in writing, since I will not be able to stay around today. Thank you very much.

[The prepared statement of Evan Hendricks follows:]

PREPARED STATEMENT OF EVAN HENDRICKS, EDITOR/PUBLISHER, PRIVACY TIMES

Mr. Chairman, Ranking Member Schakowsky, thank you for the opportunity to testify before the Subcommittee. My name is Evan Hendricks, Editor & Publisher of Privacy Times, a Washington newsletter since 1981. For the past 28 years, I have studied, reported on and published on a wide range of privacy issues, including credit, medical, employment, Internet, communications and government records. I have authored books about privacy and the Freedom of Information Act. I have served as an expert witness in litigation, and as an expert consultant for government agencies and corporations.

I am the author of the book, "Credit Scores and Credit Reports: How The System Really Works, What You Can Do."

Due to pre-existing travel plans and other commitments, I am not able at this time to provide as detailed a prepared statement as I would prefer. Please allow me to make some fundamental points.

I appreciate the opportunity to appear before the subcommittee and applaud its work on H.R. 4127. While the bill could still be improved, it at least represents an important step forward in consumer privacy protection, and underscores this Committee's desire to move our nation's policy in the right direction. Conversely, H.R. 3997 would have disastrous consequences and should be withdrawn as an inexcusable effort to weaken consumers' rights at a time that they clearly need to be strengthened.

I also applaud the underlying purpose of this hearing – to fashion a more comprehensive approach to protecting privacy. In my view, a comprehensive approach is long overdue. I am particularly happy to be sharing the panel with my distinguished colleagues from academia and industry. I believe this panel represents a hopeful potential for consensus on this all-important issue.

A Brief History

The first serious effort to establish a national privacy policy came in the early 1970s in the wake of the Watergate scandal. Sen. Sam Ervin, a longtime proponent of privacy, sought to establish a national policy by proposing a comprehensive "Privacy Act," creating rights of Fair Information Practices (FIPs) for individuals, that would apply to both the governmental and private sector.

Lobbying and politics forced Sen. Ervin to cut a deal. The result was the Privacy Act of 1974, applying only to federal agencies, and the creation of the Privacy Protection Study Commission (PPSC), a blue-ribbon panel that held hearings, studied information-privacy issues relating to most of the private sectors, and made legislative and other recommendations published in its final report.[1] The PPSC agreed that consumers needed

[1] *Personal Privacy In The Information Age: The Report of the Privacy Protection Study Commission,* (July 1977; GPO Stock No. 052-003-00395) Herein referred to as the PPSC Report.

legal protection, but recommended a sectoral approach, rather than a comprehensive one. The PPSC supported separate statutes for financial, medical and insurance records. The conclusion favoring a sectoral approach did not seem unreasonable at the time, but in hindsight, it resulted in an importance sense, of privacy being "divided and conquered" by institutional forces at the cost of individual rights. Many of the legislative proposal stemming from the PPSC's recommendations "died on the vine" in the late 1970s and were forgotten.

The result for the past three decades has been a sort of an *ad hoc*, "hit-and-miss" response driven by anecdotes. For example, when Judge Robert Bork was nominated to be a Supreme Court Justice, a local news reporter obtained his video rental records and wrote a story about his movie viewing preferences. Congress moved quickly to pass the "Video Privacy Protection Act." The *ad hoc*, sectoral approach is also driven by the Congressional committee jurisdictional issues.

The product of 30 years of *ad hoc* development of our nation's privacy policy is a growing list of Federal and State laws, some of them effective, and some not. On the federal level we have Fair Credit Reporting Act (FCRA), Gramm-Leach-Bliley (GLB), the Cable Television Privacy Act, the Telephone Consumer Protection Act (TCPA), the Children's Online Privacy Protection Act (COPPA), Health Insurance Portability and Accountability Act (HIPAA), and the Family Educational Rights and Privacy Act (FERPA).

One downside of the sectoral approach is the plethora of uneven and potentially conflicting standards for the handling of personal data. Another downside is that important types of personal data are left uncovered by law or do not appear to be clearly covered.

Of course, these shortcomings have inspired States to try to fill the gaps and to respond to fast evolving privacy issues in order to protect their citizens.

Fair Information Practices (FIPs)

Prof. Alan F. Westin, of Columbia University, was one of the early, modern-day scholars of privacy. In his 1967 book, Privacy and Freedom, he focused on the emerging issue of "information-privacy" – how the amassing of personal data allowed for new forms of "data surveillance." In the book, Westin defined privacy in part as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." Harvard Law Professor Charles Fried once referred to privacy as "that aspect of social order by which persons control access to information about themselves."

Similarly, the U.S. Supreme Court wrote, "To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[2]

The goal of providing individuals with reasonable control over their personal information led to the formulation of Fair Information Practice Principles, an effort in which Prof. Westin was integrally involved. In its 1973 report, the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems defined five principles fair information practice:

(1) there must be no personal data recordkeeping systems whose very existence is secret;
(2) there must be a way for an individual to find out what information about him is in a record and how it is used;

[2] U.S. Dept. Of Justice v. Reporters Committee, 489 U.S. 749 (1989). This definition of privacy was reaffirmed and expanded upon by the Court in Office of Independent Counsel v. Favish, 541 US 157 (2004)

(3) there must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent;
(4) there must be a way for an individual to correct or amend a record of identifiable information about him; and
(5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

One year after the 1973 report, the Watergate scandal raised the nation's privacy consciousness. Prof. Westin's book and the HEW Task Force report became the foundation for enactment of the U.S. Privacy Act of 1974. That Act, in turn in 1975 created the Privacy Protection Study Commission (PPSC), a blue-ribbon panel that held hearings, studied information-privacy issues relating to most of the private sectors, and made legislative and other recommendations published in its final report.[3]

The report's introduction articulated three objectives[4] that endorsed Fair Information Act Principles. "These three objectives both subsume and conceptually augment the principles of the Privacy Act of 1974 and the five fair information practices principles set forth in the 1973 report of the [HEW] Secretary's Advisory Committee On Automated Personal Data Systems."

The PPSC report set the foundation for analyzing and evaluating law, policy and organizational practices relating to the collection, use and disclosure of personal data. Its ***methodology*** was to ***identity the principles of Fair Information Practice*** and ***then apply them*** to the issue at hand, whether it be a standard industry practice or the statute governing that industry.

In 1980, the Organization of Economic Cooperation and Development, based in Paris, adopted the following eight principles of fair information practices, still referred to by some experts as the "Gold Standard" of privacy.

- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Participation
- Accountability

These principles were endorsed by the Governments of the United States, Japan and most Western European countries. These principles effectively have been recognized by the United Nations in its work on privacy.

These principles are at the core of major U.S. information-privacy laws, like the Fair Credit Reporting Act of 1970, and the U.S. Privacy Act of 1974. They also are at the core of the National Data Protection Laws of European countries, as well as Canada, New Zealand and Australia, and the European Union's Directive On Data Protection.

---

[3] *Personal Privacy In The Information Age: The Report of the Privacy Protection Study Commission,* (July 1977; GPO Stock No. 052-003-00395) Herein referred to as the PPSC Report.

[4] The three general principles were: (1) minimize intrusiveness; (2) open up record-keeping operations in ways that will minimize the extent to which recorded information about an individual is itself a source of unfairness in any decision about him made on the basis of it (maximize fairness); and (3) create legitimate enforceable expectations of confidentiality

FIPs: The Goal, and the Measure of Success

The extent to which we will be successful in fashioning the kind of quality law that the American people want and deserve in part will be determined by the extent we are able to incorporate all eight of these principles into the statute. Allow me to briefly explain why.

Openness = Access

The first principle of privacy/FIP is that there should be no record system whose very existence is secret. On an individual basis, Americans must have access to records about them held by major organizations. Americans have this right under the FCRA, Privacy Act and a few other laws. But because they do not have these rights in relation to many other records, there effectively are out of Americans' reach, thereby constituting a form of secret records. I salute the companies at the witness table and others that have endorsed in principle Americans right of access to records about them. It probably is the first step that legislation must tackle. Companies that have not had to implement access requirements worry that it would lead to a tsunami of requests that would overwhelm them. This has never materialized throughout recent history – even throughout 2004 and 2005 when Americans for the first time were entitled to free copies of their credit reports. Some companies also might fret that individual access might expose their proprietary data. But existing statutes are carefully worded to preclude this possibility.

Participation = Correction

A key reason why access is important is so that individuals can discover inaccurate information, dispute it, and have it corrected or removed. This goes to importance of accuracy in Fair Information Practices, ensuring that people are judged on the basis of accurate information.

Purpose Specification/Use Limitation

A fundamental precept of FIPs is that information collected for one purpose should not be collected for other purposes without the consent of the individual. Even under the FCRA and the Privacy Act, there are many allowable data uses without the individual's prior consent. The FCRA permits this by broadly specifying "permissible purposes" – i.e. credit, insurance and "legitimate business purpose." Employment is also a permissible purpose, but deemed so sensitive that it requires prior consent by the job applicant. The Privacy Act allows federal agencies to share data without consent under the "Routine Use" exception. Unfortunately, this has proven too broad a loophole that some Federal agencies are all too willing to take advantage of.

Data Quality

Data quality relates to issues that could make information less useful or unfair. This goes beyond issues of "technical accuracy." It relates to such issues as completeness and relevance, to borrow two terms from the FCRA. For example, it could be technically accurate that a landlord filed a conviction action in court against the tenant. But that would unfairly portray the tenant if it were proven the landlord's motion was frivolous and was done to retaliate against the tenant for complaining about unlivable rental conditions – as the latter information would be relevant and give a more complete picture assuring fairness. Maintaining data quality sometimes requires appropriate audits.

Security Safeguards

If information is not adequately protected, then it can be breached and privacy can be compromised. In fact, the Privacy Act requires that agencies:

> (10) establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

Moreover, Congress grafted the Privacy Act language into the security safeguards section of the Gramm-Leach-Bliley Act governing financial institutions. The problem is that aside from FTC actions, there is little enforcement of the Privacy Act or GLB security safeguards. That means organizations could calculate it is cheaper not to comply, as the chances of large fines, or other enforcement actions holding organizational heads accountable, were not great.

On their face, the Privacy Act and GLB standards seem good. But the recent litany of data breaches underscores that a duty without enforcement is not much of a duty and does not achieve its goals.

Real security requires more than just talking points. It requires leadership, good policies, employee training and awareness, encryption and intrusion detection.

Collection Limitation

This relates to collecting the minimal amount of data needed to accomplish a task. It's also referred to as data minimization, a standard under U.S. wiretap law.

This principle can relate to our discussion in two important ways. First, it relates to limiting the collection and storage of Social Security numbers (SSNs). The SSN is the identity thief's first tool of choice. Many of the publicized security breaches have been potentially traumatic because they involved (unencrypted) SSNs.

Second, it relates to encryption. If personal data, like the above-mentioned SSNs, are robustly encrypted, then even if they are lost and stolen, they are usually unusable. Thus, encryption minimizes the amount of available personal data, enhancing security and privacy.

Accountability = Enforcement

A privacy law without adequate enforcement is a right without a remedy. Unfortunately, many privacy laws suffer from lax enforcement.

It is vital to understand that when you are talking about laws affecting some 200 million people, you need to "democratize" enforcement. You can never build a bureaucracy big enough to enforce such a widely applicable privacy law – nor would you want to.

The best model for enforcement is the FCRA. It's enforcement scheme is

1) FTC & Federal Banking Agencies
2) State Attorneys General
3) Private Right of Action
    a. Statutory Damages
    b. Actual Damages
    c. Punitive Damages
    d. Attorney's fees

A privacy law cannot fully achieve its goals unless there is an adequate enforcement mechanism and that mechanism cannot be adequate if individuals do not have the ability to enforce their own rights. I'd be happy to provide the subcommittee with numerous examples.

Privacy 'Infrastructure'

The other necessary aspect of an adequate national policy is Privacy Infrastructure. This relates to having the resources in place to implement and oversee policy. We have

slowly begun building this infrastructure. For example, the statute creating the Dept. of Homeland Security created the first statutorily mandated Chief Privacy Officer. The Bush Administration last year directed Federal agencies to appoint a senior officer in charge of privacy policy. Many major corporations began appointing Chief Privacy Officers in the late 1990s.

What is missing in the U.S. is what every other Western nation has: a national office in charge of overseeing privacy policy. In other countries, they are called Office of the Privacy Commissioner or Office of Data Protection Commissioner. In some countries they have regulatory powers; in others, they do not. What is most important is that they are independent offices that typically answer to the legislative branch (the Parliament), not the executive. They typically have jurisdiction over the public and private sectors. These offices typically have limited staff, but pay great dividends in many countries because of their ability to focus attention on everything from questionable practices to emerging technologies. They also serve as a resource for the public, media and legislative and government branches.

Sen. Sam Ervin originally proposed that the United States have such an office, but politics forced him to settle for a study commission. The absence of a national office has greatly retarded the evolution and development of national privacy policy, and resulted in the hodge-podge of laws we have today. In fact, an early job for a U.S. Privacy Commissioner would be to do an accounting of what personal data of Americans actually are protected, and identify gaps and potential conflicts in existing laws.

This subcommittee should include in its legislation the creation of national privacy office. In years past, Sen. Paul Simon proposed creation of such an office. At a minimum, the office should have subpoena power and the ability to conduct audits and handle complaints. I am confident that such an office would pay great dividends for millions of Americans.

Again, thank you for this opportunity. I'd be happy to answer any questions.

MR. STEARNS. Mr. Hendricks, would you be able to stay an extra 10 minutes, because these folks will be through in 10 or 15 minutes?

MR. HENDRICKS. I will try my best, but I am sorry.

MR. STEARNS. It is interesting, your comment relative to Ms. Whitman is a little different on some of these points. I think it would be useful, some of these nuances, to talk about.

Dr. Lenard.

DR. LENARD. Thank you, Chairman Stearns, Ranking Member Schakowsky, and members of the subcommittee. I appreciate the opportunity to testify today. I am a Senior Fellow and a Senior Vice President for Research at The Progress & Freedom Foundation. We are a think tank that focuses on public policy issues that affect the information economy.

I will give a slightly different perspective than perhaps some of the other members of the panel to the issue that we are discussing. The advances in IT and finally the digital revolution have reduced the cost of gathering, storing, and manipulating information of all kinds, and this has naturally raised concerns on the part of individuals about what information is being collected, how it is being used, who has access to it, and how secure it is.

When considering whether and how to regulate, however, we need to be mindful that we truly do live in an information economy, and that the personal information utilized by firms produces great value for consumers and for the economy generally.

Moreover, regulation inevitably will have unpredictable and unintended consequences, especially when imposed on a medium like the Internet that is changing so rapidly. Perhaps the most serious potential costs involve losses of innovation.

Implicit in proposals to regulate the market for personal information is that there is a market failure resulting in too much information being produced and used, and that this is harming consumers. But despite widespread perceptions that personal information is subject to misuse, there is not much in the way of hard evidence that consumers are being harmed by the legal use of personal information.

Moreover, as a general matter, markets work better with more information. As the cost of information goes down, market participants obtain more of it and make better decisions. Indeed, increased use of personal information can correct market failures that otherwise would exist.

Regulation that raises the cost of information will result in markets that function less well and will adversely affect competition, particularly on the Internet, where established firms have listed their own customers and visitors to the Web sites, but new firms must purchase such lists. As long as there is a market for such information, entrants can begin competing relatively easily.

However, if regulation reduces the size of the market and increases costs, competition from new entrants will be reduced. The market also appears to provide incentives for firms to respond to consumers' privacy concerns in a variety of ways, including voluntary standards and new technologies such as spam filters. Firms that violate consumers' expectations about privacy face a loss of reputation that translates into losses in the marketplace.

Data security and identity fraud present a slightly different issue, because they deal with behavior that is illegal. Again, contrary to the public perception, this is not a growing problem. Indeed, identity fraud costs are, by most measures, declining. This should not be surprising, because about 90 percent of the costs are borne directly by businesses which, therefore, have a strong incentive to invest in security, and reduce these costs.

Businesses may not necessarily have the same incentives to notify in the event of a security breach, but our analysis indicates that a mandatory notification is somewhat dubious on cost-benefit grounds. The indirect costs both to consumers and to sectors of the economy that depend on the

free flow of information are likely to be substantial, primarily because of a likelihood that both consumers and firms suffering a security breach will overreact to notification requirements.

Whatever privacy and data security regulation we do adopt, however, should be at the Federal level and preempt State laws. The effective markets are national and international in scope. Federal preemption will reduce compliance costs and improve the benefit-cost balance.

The privacy debate represents some of the most complex policymaking challenges that we have seen. This requires a careful analysis of specific proposals and their likely consequences to assure that their benefits are sufficient to justify their costs. Thus far, the evidence suggests the market for personal information is working pretty well and producing large benefits for consumers.

Regulating in this rapidly changing technological environment, without evidence of significant market failure, runs the risk of adversely affecting innovation and slowing the progress of the IT revolution with potentially adverse implications for growth and productivity.

Thank you very much.

MR. STEARNS. Thank you.

[The prepared statement of Dr. Thomas M. Lenard follows:]

PREPARED STATEMENT OF DR. THOMAS M. LENARD, SENIOR VICE PRESIDENT FOR RESEARCH, THE PROGRESS & FREEDOM FOUNDATION

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Thomas Lenard. I am senior fellow and senior vice president for research at The Progress & Freedom Foundation, a non-partisan, non-profit "think tank" that focuses on public policy issues that affect the digital revolution and the information economy generally. Privacy and data security are clearly among the most important of these issues.

The advances in information technology that define the digital revolution have reduced the costs of gathering, storing, manipulating and transmitting information of all kinds. While the economic and social impacts of these advances have been overwhelmingly positive, they also have raised concerns on the part of individuals about what information is being collected, how it is being used, who has access to it and how secure it is. These concerns have been exacerbated by a series of high-profile data-security breaches that have exposed millions of individuals to potential fraud and convinced much of the public that we face an epidemic of identity theft.

When considering whether and how to regulate, however, we need to be mindful that we truly do live in an information economy and that the personal information utilized by firms produces great value for consumers and the economy. It is the reason, for example, why any individual with a decent credit rating can get a loan approved virtually instantaneously. It also facilitates competition generally, making it easier for new firms to enter markets that require customer data. It is an area where the United States has a significant advantage over other countries that have more restrictive data and privacy laws and where consumer credit markets and other markets that rely on personal information don't work as smoothly.

Moreover, regulation will inevitably have unpredictable and unintended consequences, especially when imposed on a medium like the Internet that is changing so rapidly. Perhaps the most serious potential cost is a loss of innovation—new uses of information and of the Internet itself that would be frustrated by a new regulatory regime. There are many examples of ways in which information is now being used that were not contemplated when the information was collected, and which would be precluded by some of the measures that have been proposed.

In deciding whether additional regulation is desirable, and, if so, in what form, the following basic public policy questions need to be addressed:[1]

- Are there "failures" in the market for personal information?
- If market failures exist, how do they adversely affect consumers?
- Can such failures be remedied by government action?
- Will the benefits of government regulation exceed the costs?

The Market for Personal Information

Although privacy and data security are obviously inextricably intertwined, it is useful to think of them separately for the purposes of regulatory analysis. So, the first question is whether there are failures in the market for information and, in particular, whether consumers are being harmed by the legal use of personal information for commercial purposes. The answer is that, despite widespread perceptions that personal information is subject to misuse, there does not appear to be much in the way of evidence, even anecdotal evidence, of such harm.

Implicit in the proposals to regulate the market for personal information is that there is a market failure resulting in "too much" information being produced, disseminated and used. As a general matter, however, markets work better with more information. As the cost of information goes down, market participants obtain more of it and, consequently, make better decisions. For example, consumers benefit from receiving information that is better targeted to their interests, as well as from not receiving information that is not of interest to them. Similarly, legitimate marketers have an interest in not sending messages to consumers who aren't interested in them. Merchants with more information can better estimate demand, reducing inventory costs and even lessening swings in overall economic activity. They can also use geographic computer-based information to put their new stores in locations that best serve consumers, and to stock the most useful merchandise for those consumers.

Information can correct market failures that would otherwise exist. For example, asymmetric information is a form of market failure that occurs when one party to a transaction has more information than the other. Both credit markets and insurance markets are potentially subject to problems of this sort, because lenders and insurers may have less information than applicants about the applicants' risk characteristics. Asymmetric information problems of this sort may cause lenders and insurers to be unwilling to offer transactions that consumers would want and that would benefit them. In general, increased use of personal information alleviates, rather than exacerbates, this type of market failure.

Moreover, the "public good" nature of information—once produced, it can be reused multiple times—means that advertisers, credit institutions and insurance companies all may use the same information. The ability to sell for advertising or marketing purposes information initially collected for credit or insurance rating purposes increases the value of that information. Thus, the markets for advertising and marketing information

[1] For an elaboration of many of the points made in this testimony, see Paul H. Rubin and Thomas M. Lenard, *Privacy and the Commercial Use of Personal Information*, Kluwer Academic Publishers and The Progress & Freedom Foundation, 2002.

generate increased information in markets that might truly be susceptible to asymmetric information market failures—e.g., credit and insurance markets.

The market also appears to provide incentives for firms to respond to consumers' privacy concerns in a variety of ways. Firms that violate consumer expectations about privacy face a loss of "reputation" that translates into losses in the marketplace. When a firm does something that is perceived as harming its reputation with consumers, the firm suffers a substantial loss in value. Firms, therefore, have a strong incentive to avoid undertaking policies that risk offending their customers. The Internet speeds the collection of information about consumers, but it also enables consumers to more easily obtain information about firms' activities on the Web. In addition, voluntary standards, defined and enforced by third parties or consortia of Web operators, are an important mechanism for providing information to consumers about Web sites' information policies. Finally, new technologies, such as spam filters, are available to consumers who are concerned about privacy.

Data Security

Data security presents a slightly different issue. While there may be no evidence of market failure or consumer harm from the legal use of personal information in commercial markets, that does not necessarily imply that firms have the appropriate incentives to safeguard the information under their control or take appropriate steps, whatever these may be, if the data are compromised.

The most recent data on identity theft and its costs (from a 2006 report from Javelin Strategy and Research) do not support the public perception that identity theft is a growing problem. They show that the costs of identity fraud have been essentially constant over the last several years for which data are available (which would indicate that, in a growing economy, they have been declining relative to total transactions). Since 2003, the number of victims of identity fraud has declined by almost 12 percent—to 8.9 million annually—while the average cost per victim has increased by over 20 percent. However, since most victims don't incur the costs related to their fraud cases, the average consumer costs have declined by 24 percent, although the time it takes consumers to resolve fraud cases has increased from 33 to 40 hours.

Other data suggest that costs have been decreasing over time. Estimates by Nilson show that over a longer period—1992 to 2004—the costs of credit card frauds decreased from $0.157 to $0.047 per $100 in credit card sales.[2] Similarly, Visa recently indicated that its fraud costs are at an all-time low of five cents per $100 of transactions. This is a reflection of the fact that credit card firms are continually updating and improving levels of security. The Nilson Report also indicates that fraudulent charges are lower as a percentage of credit card use in the U.S. than in the rest of the world; for example, credit card payments in the U.S. are three times the U.K. level, as compared with fraudulent charges, which are only about 1.2 times the U.K. level.

It shouldn't be surprising that fraud costs per dollar of transaction are declining. About 90 percent of the costs of identity theft and related frauds are borne directly by businesses, including banks, credit card issuers and merchants. In addition, studies show that firms suffer large losses in stock value when security is breached. Interestingly, these studies are from a period before any consumer notification was required. Despite the perception that information about security breaches was unavailable prior to enactment of the California notification requirement, information about breaches did become public before that time—perhaps as a result of securities regulatory requirements—and markets reacted accordingly. Thus, even without any laws mandating notice to consumers, firms have had a very strong incentive to avoid data security breaches because the market penalizes them severely.

---

[2] These figures are for costs to card issuers.

It is unclear whether firms also have adequate incentives to notify compromised consumers, so the issue is an empirical one: do the benefits of notification outweigh the costs? This issue was addressed in an economic analysis of notification requirements for data security breaches I recently did with Paul Rubin, who is a professor of law and economics at Emory University as well as an adjunct PFF fellow.[3]

We found that a notification requirement is dubious on benefit-cost grounds. The expected benefits to consumers of such a requirement are extremely small—probably under $10 per individual whose data have been compromised. There are several reasons for this. First, most cases of identity theft involve offline security breaches, which are not affected by notification requirements. Second, the probability of an individual compromised by a security breach becoming an identity-theft victim is extremely small. Third, most of these are victims of fraudulent charges on their existing credit accounts, for which they have very limited liability, rather than victims of true identity theft. Finally, even a well-designed notification program is likely to eliminate only a small fraction of the expected costs.

While the direct costs of notification may not be large, the indirect costs both to consumers and to sectors of the economy that depend on the free flow of information are likely to be substantial, primarily because of the likelihood that both consumers and firms suffering a security breach will overreact to notification. Firms in the information business may start limiting access to their information in an effort to reduce their risk exposure. Of particular concern is the prospect that the publicity associated with multiple notifications may induce consumers to shift their credit transactions offline, which the data show would actually increase their exposure to identity theft.

Effect on Competition

Many of the costs of privacy and data security regulations are likely to be relatively invariant with the size of the firm and therefore higher per unit of output for small than for large firms. Many of the costs are also what economists call "sunk" costs, which means they are not recoverable if, for example, the business fails. This is an added burden that will deter start-ups and could have an adverse effect on competition.

Most importantly, any regulation of the information sector that raises the costs of targeted advertising and obtaining accurate customer lists has a greater adverse effect on new entrants and small firms than it does on large, established firms. This is particularly true for Internet advertising, where established firms have lists of their own customers and visitors to their web sites, but new firms must purchase such lists. As long as there is a market for customer lists and other such information, entrants can begin competing relatively easily. However, if regulation should reduce the size of the market and increase costs, competition from new entrants would be reduced.

Federal vs. State Regulation

Given the nature of the Internet, regulation at the state level has the potential to produce additional costs and impede interstate commerce due to inconsistencies. A true federalist approach is not possible with markets and firms that are national, and even international, in scope. Firms will tend to comply with a single set of rules. In the absence of a preemptive federal statute, they will comply with the most stringent set of state regulations, which will in effect "preempt" other state regulations.

Without federal preemption, companies are still faced with the prospect of familiarizing themselves with numerous different state laws to make sure they are in compliance. The costs associated with this, which do not vary much with firm size,

---

[3] Thomas M. Lenard and Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," The Progress & Freedom Foundation, *Progress on Point*, Release 12.12, July 2005.

constitute a particular burden for smaller firms. Federal preemption of state privacy and data-security laws will reduce compliance costs and improve the benefit-cost balance.

Conclusion

The privacy debate represents some of the most complex policy-making challenges we have seen. This requires careful analysis of the actual proposals and their likely consequences to assure that, if adopted, their benefits are sufficient to justify their costs. Thus far, and despite perceptions to the contrary, the evidence suggests that the market for personal information is working well and producing large benefits for consumers. Regulating in this rapidly changing technological environment, without evidence of significant market failure, runs the risk of adversely affecting innovation and slowing the progress of the IT revolution, with potentially adverse implications for growth and productivity.

MR. STEARNS. Professor Swire.

MR. SWIRE. Thank you, Mr. Chairman, Ranking Member Schakowsky, and members of the committee. Thank you very much for the invitation to testify here before you today on the subject of Federal consumer privacy legislation.

My name is Peter Swire. I am the C. William O'Neill Professor of Law at The Ohio State University, home of the Buckeyes. Today I am representing the Consumer Privacy Legislation Forum. To summarize the testimony, increased use and access to information, often made possible by advances in technology, have greatly benefited society through the exchange of ideas, enhanced economic productivity, and increased access to goods and services.

Without the appropriate safeguards, however, access to information can pose potential harm to consumers, resulting in a general lack of confidence that their information is safe. Unaddressed, a loss of trust has an adverse impact on economic growth and innovation.

I became aware of the promise and perils of information uses when I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget from 1999 until early 2001. While at OMB, I worked on issues such as on-line privacy, medical privacy and financial privacy. I also oversaw the Federal government's use of personal information. We were subject to the Privacy Act and other legal requirements, so I learned what it is like to be regulated.

From that experience, I came away with a keen appreciation for the benefits and protections that come from good privacy laws. I also saw, however, the serious problems that can arise if privacy rules are not crafted carefully.

The CPL Forum, whose creation we are announcing today, grew out of an announcement last fall by eBay, Hewlett-Packard, and Microsoft, that they supported a national standard for privacy protection that will benefit consumers, while allowing commerce to flourish. These

companies, along with the Center for Democracy and Technology and myself, have become the steering committee for our Forum.

It is an honor and privilege today to be appearing at this hearing alongside Ms. Meg Whitman, the CEO and President of eBay Inc., and Mr. Scott Taylor, the CPO of Hewlett-Packard. Both Ms. Whitman and Mr. Taylor today are giving the perspective of their respective companies, and there may be specific items where the Forum as a group has not yet settled into a position.

Having their personal participation, including at the CEO level, underscores the importance of the issue of comprehensive consumer privacy legislation. Since the late winter, an expanded group of organizations has come together into the Forum to work on the topic of comprehensive consumer privacy legislation.

The list of companies signing on to the Forum's statement today is a significant moment, showing the expanded number and range of industry leaders who are stepping forward on this issue. In addition to the companies that are explicitly signing the statement, we are calling this the CPL Forum because we have reached out to and will continue to learn from a much broader array of experts and stakeholders, both on the industry and the consumers' side.

The forum has been working on more detailed principles that would inform comprehensive consumer privacy legislation. We hope and expect to have additional materials for public release in the future.

I will now turn to the formal statement that we are making today for the Forum. Here is the statement in support in principle for comprehensive privacy legislation.

Quote: "Today we live in a digital economy where both beneficial and potentially harmful uses of personal information are multiplying. Information about individuals is used by businesses to provide consumers with an unprecedented array of goods and services; increase productivity; promote access to financial products; and protect individuals, business, and society from fraud and other bad acts. However, that same information can also be misused to harm individuals, with results such as identity theft, deception, unwarranted intrusion, embarrassment and loss of consumer confidence."

"The time has come for a serious process to consider comprehensive harmonized federalized privacy legislation to create a simplified, uniform, but flexible framework. The legislation should provide protection for consumers from inappropriate collection and misuse of their personal information, and also enable legitimate businesses to use information to promote economic and social value. In principle, such legislation would address businesses collecting personal information from consumers in a transparent manner with appropriate notice;

providing consumers with meaningful choice of the use and disclosure of that information; allowing consumers reasonable access to personal information they had provided; and protecting such information from such misuse or unauthorized access. Because a national standard would preempt laws, a robust standard is warranted."

That is our statement today, as signed by 12 companies. In my written testimony, I explained some reasons the forum believes this process should be done now, why now is the time to move forward.

But given the time, I will simply conclude today by thanking the committee for once again showing leadership on consumer privacy issues by calling this hearing today. We appreciate being called to testify and pledge to work diligently to assist you in your continued consideration of these important issues.

MR. STEARNS. Thank you.

[The prepared statement of Peter Swire follows:]

PREPARED STATEMENT OF PETER SWIRE, C. WILLIAM O"NEILL PROFESSOR OF LAW, MORITZ COLLEGE OF LAW, THE OHIO STATE UNIVERSITY

Mr. Chairman, Ms. Ranking Member, thank you very much for the invitation to testify before you today on the subject of federal consumer privacy legislation. My name is Peter Swire. I am the C. William O'Neill Professor of Law at the Ohio State University, and today I am representing the Consumer Privacy Legislation Forum.

To summarize the testimony, increased use and access to information, often made possible through advances in technology, has greatly benefited society through the exchange of ideas, enhanced economic productivity, and increased access to goods and services. Without the appropriate safeguards, however, access to information can pose potential harms to consumers, resulting in a general lack of confidence that their information is safe. Unaddressed, a loss of trust has an adverse impact on economic growth and innovation.

I became aware of the promise and perils of information uses when I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget from 1999 until early 2001. While at OMB, I worked on issues such as online privacy, medical privacy, and financial privacy. I also oversaw the federal government's own use of personal information. We were subject to the Privacy Act and other legal requirements, so I learned what it feels like to be regulated. From that experience, I came away with a keen appreciation for the benefits and protections that come from good privacy laws. I also saw, however, the serious problems that can arise if privacy rules are not crafted carefully.

The CPL Forum, whose creation we are announcing today, grew out of the announcement last fall by eBay, Hewlett-Packard, and Microsoft that they supported a national standard for privacy protection that will benefit consumers while allowing commerce to flourish. Those companies, along with the Center for Democracy and Technology and myself, have become the Steering Committee for the CPL Forum. It is an honor and privilege today to be appearing at this hearing alongside Ms. Meg Whitman, the CEO and President of eBay, Inc. and Mr. Scott Taylor, the Chief Privacy Officer of Hewlett-Packard. Both Ms. Whitman and Mr. Taylor today are giving the perspectives of their respective companies, and there may be specific items where the Forum as a group has not settled into a group position. Having their personal participation, including at the

CEO level, underscores the importance of the issue of comprehensive consumer privacy legislation.

Since the late winter, an expanded group of organizations has come together into the Forum to work on the topic of comprehensive consumer privacy legislation. The list of companies signing onto the Forum's statement today is a significant moment, showing the expanded number and range of industry leaders who are stepping forward on the consumer privacy issue. In addition to the companies that are explicitly signing the statement, we are calling this the CPL *Forum* because we have reached out to, and will continue to learn from, a much broader array of experts and stakeholders, both on the industry and consumer sides. The Forum has been working on more detailed Principles that would inform comprehensive consumer privacy legislation. We hope and expect to have additional materials for public release in the future.

Let me now turn to the formal Statement of the CPL Forum that we are releasing today.

Statement of Support in Principle for Comprehensive Consumer Privacy Legislation

"Today we live in a digital economy where both beneficial and potentially harmful uses of personal information are multiplying. Information about individuals is used by businesses to: provide consumers with an unprecedented array of goods and services; increase productivity; promote access to financial products; and protect individuals, business and society from fraud and other bad acts. However, that same information can also be misused to harm individuals, with results such as identity theft, deception, unwarranted intrusion, embarrassment, and loss of consumer confidence."

"The time has come for a serious process to consider comprehensive harmonized federal privacy legislation to create a simplified, uniform but flexible legal framework. The legislation should provide protection for consumers from inappropriate collection and misuse of their personal information and also enable legitimate businesses to use information to promote economic and social value. In principle, such legislation would address businesses collecting personal information from consumers in a transparent manner with appropriate notice; providing consumers with meaningful choice regarding the use and disclosure of that information; allowing consumers reasonable access to personal information they have provided; and protecting such information from misuse or unauthorized access. Because a national standard would preempt state laws, a robust framework is warranted."

That is our statement today, as signed by 12 companies. Before closing, let me briefly indicate four reasons why members of the Forum believe that this process for federal privacy legislation should occur now.

First, it is important to promote consumer trust. A nationwide survey released in May 2006 by the Cyber Security Industry Alliance reports that 94 percent of people polled cite identity theft as a serious problem and only 24 percent feel that businesses are placing the right emphasis on protecting information.

Second, address the patchwork. Comprehensive federal consumer privacy legislation can unify today's inconsistent and incomplete patchwork of obligations at both the state and federal levels. This approach would simplify compliance for companies while at the same time providing uniform, meaningful, and understandable protections for individuals.

Third, fill the gaps. Many organizations have already developed effective privacy policies. Bad or careless actors, however, do not have the same policies in place, undermining consumer trust.

Fourth, provide an understandable U.S. framework. Compared with the current patchwork, comprehensive federal consumer privacy legislation can be more easily understood by entities and persons both inside and outside of the United States. In a

global world of e-Commerce, this simplified and understandable privacy framework helps consumers and businesses.

In conclusion, this Committee is once again showing leadership on consumer privacy issues by calling this hearing today. We thank the Committee for the invitation to testify, and pledge to work diligently to assist you in your continued consideration of these important issues.

Appendix to Swire Statement

Statement of Support in Principle for Comprehensive Consumer Privacy Legislation

Today we live in a digital economy where both beneficial and potentially harmful uses of personal information are multiplying. Information about individuals is used by businesses to: provide consumers with an unprecedented array of goods and services; increase productivity; promote access to financial products; and protect individuals, business and society from fraud and other bad acts. However, that same information can also be misused to harm individuals, with results such as identity theft, deception, unwarranted intrusion, embarrassment, and loss of consumer confidence.

The time has come for a serious process to consider comprehensive harmonized federal privacy legislation to create a simplified, uniform but flexible legal framework. The legislation should provide protection for consumers from inappropriate collection and misuse of their personal information and also enable legitimate businesses to use information to promote economic and social value. In principle, such legislation would address businesses collecting personal information from consumers in a transparent manner with appropriate notice; providing consumers with meaningful choice regarding the use and disclosure of that information; allowing consumers reasonable access to personal information they have provided; and protecting such information from misuse or unauthorized access. Because a national standard would preempt state laws, a robust framework is warranted.

CPL Forum members signing the statement today, June 20, 2006, are:

Eastman Kodak Co.
eBay Inc.
Eli Lilly and Co.
Google, Inc.
Hewitt Associates
Hewlett-Packard Co.
Intel Corp.
Microsoft Corp.
Oracle Corp.
Procter & Gamble Co.
Sun Microsystems, Inc.
Symantec Corp.

MR. STEARNS. Mr. Taylor.

MR. TAYLOR. Mr. Chairman, Ranking Member Schakowsky, distinguished committee members. My name is Scott Taylor, and I am the Chief Privacy Officer at Hewlett-Packard Company. HP is a leading global provider of computing and imaging products, services and solutions. We operate in over 170 countries worldwide. We are

headquartered in Palo Alto. We have 150,000 employees and revenues of $88 billion.

Respecting our customers' privacy has been an integral part of HP's success over the years. I very much appreciate the opportunity to share with you today HP's view on the importance of Congress considering a unifying, workable, and comprehensive Federal privacy standard.

I would like to share three important messages. First and foremost is that privacy is actually a core value at HP. We firmly believe that the ability to succeed in the marketplace depends on keeping our customers' trust, and only by ensuring the privacy and the security of the personal information that we collect about our customers can we rightfully gain and maintain that trust.

Consumers who purchase any one of the 10,000 products that HP produces must be confident not only in the quality of those products, but that we are going to do right by them, especially when it comes to protecting the personal information that we collect about them.

The second message is that HP has long been a leader in strengthening consumer privacy protections. We have a lengthy track record of advancing forward-looking workable privacy initiatives that respond to consumer needs. HP was the first U.S. company certified by the Department of Commerce to participate in the European Union's safe harbor program back in 2001.

Our global Web site, hp.com, posts a privacy statement on every one of our 4.5 million pages, as well as privacy notices at every personal data collection point. We are also active in efforts outside of our company. HP was a founding sponsor of the Better Business Bureau's BBB online program, which was one of the earliest and today one of the most internationally recognized privacy protection self-certification programs.

Finally, as Mr. Swire mentioned, HP was one of three U.S. companies who last fall launched the Consumer Privacy Legislation Forum, a group focused on advancing a national dialogue on a workable, responsive Federal privacy standard.

This brings me to my third and final point. HP does believe that it is time for Congress to consider a unifying Federal privacy law. As a leader in e-commerce, HP is a strong proponent of corporate effective regulation. We believe the future of e-commerce is dependent upon companies acting responsibly to advance consumers' needs.

At the same time, however, we recognize that consumer privacy presents a series of challenges that have not yet been fully addressed. For example, the patchwork of privacy regulations in existence today across numerous State statutes means that consumers are confused as to the extent of their protections in any given context.

Companies also have to contend with that patchwork of quilts and laws and their very differing, often conflicting regulations that we need to interpret. Further, there are heightened consumers' concerns about existing privacy threats, risks undermining the health of e-commerce. And no one is served, not consumers, not governments, and certainly not companies, by a lack of confidence in the security and privacy of personal information.

All of this adds up to one thing. We believe at HP that Congress should take steps to consider a comprehensive, Federal approach to protecting consumers' privacy, one that provides a workable national standard in lieu of the current patchwork of laws.

I would like to be clear that HP is not looking for Congress to dictate the terms or the technologies for protecting privacy. That would be counterproductive and self-defeating. Rather, we are urging Congress to examine ways of establishing a workable, flexible benchmark that unifies the divergent laws and regulations that are in existence and at the same time responds to the very real needs of anxious consumers.

We recognize that this is likely to be a multiyear effort, one that is going to require careful study and consideration by this committee and Congress as a whole. But we also believe it is a process that is well worth embarking upon.

At HP, we stand ready to serve as a resource to you, so that working together we may find meaningful, functional ways to protect the privacy of the American consumer and realize the full potential of e-commerce.

Thank you.

[The prepared statement of Scott Taylor follows:]

PREPARED STATEMENT OF SCOTT TAYLOR, CHIEF PRIVACY OFFICER, HEWLETT-PACKARD COMPANY

Mr. Chairman, Ranking Member Schakowsky, and distinguished Committee members, my name is Scott Taylor and I am the Chief Privacy Officer for Hewlett-Packard Company.

Headquartered in Palo Alto, California, HP is a leading global provider of computing and imaging solutions and services, conducting business in over 170 countries around the world with 150,000 employees globally and revenues of $88 billion. Respecting our customers' privacy has been in our DNA since the inception of the company and an integral part of our success. I very much appreciate the opportunity to share with you today our views on the importance of Congress considering a unifying, workable and comprehensive Federal privacy standard.

I want to leave you with three important messages today:

- **First, privacy is a core HP value.** We firmly believe that our ability to succeed in the marketplace depends upon earning and keeping our customers' trust. Only by ensuring the privacy and security of all the customer information that we handle can we rightfully gain and maintain that trust.
- **Second, HP has long been a leader in corporate efforts to strengthen consumer privacy protections globally**. From becoming the first U.S.

company to participate in the EU's Safe Harbor program back in 2001, to having helped launch the Consumer Privacy Legislation Forum last fall, HP has a lengthy track record of advancing forward-looking, workable privacy initiatives that respond to consumer needs.

- **And finally, in keeping with that record of leadership, HP believes it is time for Congress to consider establishing a comprehensive, flexible, and harmonized legal framework for protecting consumer privacy.** Consumers want it, companies need it, and our economy will be the better for it.

Let me briefly address each of these points.

First and foremost, privacy is a core HP value.

As a company, HP is 100 percent committed to excellence in consumer and employee privacy, and for two fundamental reasons.

First, because it's the right thing to do. We have an obligation to fulfill the trust that HP employees have given us in handling their information

Second, because successful customer relationships are fundamentally about *trust*. Consumers who purchase any one of the 10,000 computer and imaging products produced by HP must be confident not only in the quality of our products, but in the integrity of their customer experience. They must trust that we will do right by them, particularly when it comes to protecting the privacy and security of their personal information.

It is for this reason that HP operates one of the most rigorous global privacy policies of any major U.S. company. In fact, in January 2005, TRUST*e* and the Ponemon Institute named HP "The Most Trusted Company in America for Privacy."

Secondly, HP has long been a leader in strengthening consumer privacy protections.

In fact, we've been at the forefront of corporate efforts to strengthen global privacy protections for many years now.

First, a bit about our own policies. HP's global website, www.hp.com, posts a privacy statement on every page as well as privacy notices at every personal data collection point. We offer a range of pro-consumer privacy protections for users, including choices about marketing contact preferences and an opt-in approach for sharing personal information with third parties outside our company. My position -- Chief Privacy Officer -- is charged with ensuring that HP's global privacy policies match the highest standards of privacy excellence everywhere in the world.

We are also active in efforts to advance dialogs on privacy issues outside our company. HP was a founding sponsor of the Better Business Bureau's BBB*OnLine* Program, one of the earliest and, today, most internationally recognized privacy protection self-certification programs.

In 2001, we became the first American company certified by the Department of Commerce to participate in the European Union's Safe Harbor program. Our global privacy policy is, in fact, based on the Safe Harbor, a rigorous standard designed to be compatible with the European Union's high data privacy requirements.

And finally, HP was one of three U.S. companies who last fall launched the Consumer Privacy Legislation Forum – a group of privacy-minded companies and consumer organizations focused on advancing a national dialogue on a workable, responsive Federal privacy standard.

Which brings me to my final point:

HP believes it is time for Congress to consider a unifying Federal privacy law.

As a leader in e-commerce, HP is a strong proponent of effective corporate self-regulation. We believe that the future of e-commerce depends on companies acting responsibly to advance consumer needs.

At the same time, however, we recognize that consumer privacy presents a series of challenges that have not yet been fully addressed. For example, the patchwork of state-based privacy regulations in existence today with many different statutes means that consumers are confused as to the extent of their protections in any given context, and that companies must contend with a mix of differing and often conflicting regulations.

Further, heightened consumer concerns about existing privacy threats – from spyware to phishing, spam to data breach, and any number of other challenges – risk undermining the economic health of e-commerce. No one is served – not consumers, not governments, and certainly not corporations – by a lack of customer confidence in the security and privacy of personal information.

Which adds up to one thing:

HP believes that Congress should take steps to consider a comprehensive federal approach to protecting consumer privacy – one that provides a workable *national* standard in lieu of the current patchwork of state laws. This national baseline should be built on fundamental, sound privacy principles that include:

- transparency and consumer choice;
- scalability and flexibility;
- information security;
- accountability; and
- strong enforcement.

Let me be clear: we are not looking for Congress to dictate the terms *or technologies* for protecting privacy. That would be counter-productive and self-defeating. Rather, we are urging Congress to examine ways of establishing a workable, flexible benchmark that unifies the divergent regulations currently in existence and, at the same time, responds to the very real needs of anxious consumers.

We recognize that this is likely to be a multi-year effort – one that will require careful study and consideration by this Committee and by the Congress as a whole. But it is a process that we believe is well worth embarking upon.

At HP, we stand ready to serve as a resource to you, so that working together, we may find meaningful, functional ways to protect the privacy of American consumers and realize the full potential of e-commerce.

Thank you.

MR. STEARNS. I thank you, all of you. I will start with my questions.

Ms. Whitman, I will start with you, with your background. It is nice to see you again. I had an opportunity some time ago to tour eBay, and I remember that vividly.

Almost everybody on the panel has indicated we need a comprehensive bill, and we need a Federal bill. Mr. Hendricks, though, has pointed out, though, he does not want to see a private right of action in his opening statement.

Ms. Whitman, you had indicated--he does want one and you do not.

MS. WHITMAN. Yes.

MR. STEARNS. Having seven hearings on privacy before, it always has been a problem trying to reach a compromise. I think it would be important for you, you have this opportunity now to say how you feel on this subject, and I was hoping Mr. Hendricks would give his opinion, but I am sure maybe someone else will contribute his, but we welcome your thinking here for the record.

MS. WHITMAN. Thank you very much. Our point of view is that the FTC has, in fact, led the charge to protect consumer privacy, and so we believe it is the right enforcement body. Also a private right of concern, I think our biggest concern is that this could lead to an onslaught of plaintiff bar class action lawsuits that would potentially inconsistently enforce privacy legislation and also lead to just enormous legal complexity and legal costs on behalf of companies.

MR. STEARNS. The argument often goes, though, that if you don't have private right of action, you don't get punitive and civil damages, which a lot of people would say individual consumers should have the individual right, if there is a compromise here by a large corporation.

Mr. Taylor, you are welcome to pitch in here. But how would you answer that; with the Federal Trade Commission, perhaps, there is not the full rights of an individual consumer to have civil and punitive damages?

MS. WHITMAN. You know, that may be the case. I think the issue here is what is the right balance. We certainly want to, as I said in my opening statement, have a very well-enforced baseline, transparent, consumer privacy protection.

At the same time, I think we also want to be fair to all the constituencies and make sure that this doesn't get so complicated that the very best companies are, if you will, just brought to their knees by enormous lawsuits and potential damages. So I think it can be under discussion, but I think we are just trying to find the right balance here in terms of what the right enforcement mechanism is.

MR. STEARNS. Mr. Taylor, you might want to comment, and I was going to ask Professor Swire what his comments were.

MR. TAYLOR. I would agree with Ms. Whitman that we need to have a fundamental baseline that has flexibility and scalability, because I would agree with her that it is important that we don't grind this to a halt and make this too complex.

MR. STEARNS. You support full preemption, then, as opposed to the private right of action. Can you go on record and say, or are you saying it is more nuanced than that; that maybe there could be a compromise, using a State Attorney General enforcement?

MR. TAYLOR. Yes, I would say there could be a compromise.

MR. STEARNS. Professor Swire.

MR. SWIRE. In terms of me being here for the CPL Forum today, maybe being a plain law professor for a second I can point out we have statutes that have a variety of things, so we can look at those. We have had the FCRA, which has had a private right of action since 1970. We have HIPAA, which is only Federal enforcement.

You all might have seen a front-page story in the Washington Post a couple of weeks ago that shows there hasn't yet been the first civil enforcement action 3 years after that got in play. That is an example of a Federal-only statute.

In the CAN-SPAM statute that came out of this committee, State AGs have a role, and also some particular companies that basically stand in for the Internet, the ISPs, have a role. So we have a variety of statutes to look at. I think you can study how each of those has worked out.

MR. STEARNS. Ms. Whitman, another area I find of contention is the level of correction and notice that is in a rebus notice. It is a notice that is sort of a limited notice? How do you feel about this? The notice to the consumer in the event there is a problem, notice to the consumer advising that he or she, that their privacy--and then the consumer calls you. Just like my credit report, I can get it corrected; I can get a free copy. How do you feel about that, the level of notice and the ability of the consumer to get this corrected?

MS. WHITMAN. One of the proposals I think we subscribe to is transparency. I think notice is incredibly important. I guess the nuance is if there has been a tiny two or three people, their information has been compromised, obviously you would notify those people, you would notify a very large group of people. But is there some case where it doesn't make sense to notify?

I think our bias at eBay, if there is ever a breach, no matter how small, that one must notify the consumers and make sure that you either reach them by phone, by email, or by snail mail, hand-based letter. I think we do feel that notification and transparency are incredibly important because that allows consumers to take their own precautions, canceling their credit cards, whatever they would like to do.

With regard to access, we do believe that consumers should be able to access their open information so far as the access is balanced, I think, with a reasonable standard. But I think it is every consumers right to know what has happened with that information, and we ought to make ourselves available to consumers to be able to find out what we have about them that maybe they didn't understand in our privacy policies.

MR. STEARNS. That is a very important point. Let us say I have been doing business with you for 10 years. I say, I would like to say what eBay has on me. Are you receptive to a procedure where I could notify you and see to eBay, please give me records of what you have as

far as personal information on me, and you are receptive as a corporate CEO to say we are willing to live with that extra, perhaps, nuisance; or, even though there has been no notice and there has been no violation, but the person just wants to call?

MS. WHITMAN. Yes, I think with a reasonableness test, we would be open to that. The most important information that we have about consumers, of course, is in some ways their reputation that they build on eBay. We keep that forever.

We now have over, I think, 70 billion feedback comments from our buyers and sellers. People can access that at all times. We would be happy to provide them basically with any information they want, subject to probably some minor reasonableness tests. But I think that is an absolutely legitimate request.

MR. STEARNS. Do you agree, Mr. Taylor? I think she is stretching out here. I don't think the corporations--we had other hearings, and they are not all receptive to everybody having access to see what their records are without a notice, without any problems.

MR. TAYLOR. HP does work very hard to allow access to information. One of our privacy principles is data access. Of course, like Ms. Whitman said, it is as reasonable an access as we can provide. When consumers contact us, we do have a privacy mechanism to allow a general consumer to contact HP to question the content or data.

MR. STEARNS. So you are willing to go as far as the credit unions?

MR. TAYLOR. I don't know if we are as willing to go or willing to go as far as the credit unions.

MR. STEARNS. In other words, I can call up any credit union and say, tell me what you have got; or I can call up any credit union and find out in the credit report.

MR. TAYLOR. In our case what we will do is if a consumer asks us to view their information, change their information, we will make our best attempt in the variety of databases to look for all active information that might be used, or active, about that user.

MR. STEARNS. You would want the Federal government to put that into legislation? Would that bother you?

MR. TAYLOR. I think reasonable access on behalf of consumers to information that companies have would not be an unreasonable request.

MR. STEARNS. All right. My time has expired. Ms. Schakowsky.

MS. SCHAKOWSKY. Thank you. I am really impressed with our panelists.

Ms. Whitman, I know friends who live on eBay and make a living in some part on eBay. It is a pleasure to hear you.

I wanted to get to this issue of preemption also, and, Professor Swire, you said that because the setting of a national standard for privacy would preempt State laws, that a robust framework is warranted.

In the preemption that you are imagining, would there be any room for States to go beyond the Federal legislation should we miss something?

MR. SWIRE. Well, within this Forum, this group that we have been working with, the Center for Democracy and Technology and the dozen companies that have signed on in a bigger group that we have been talking with, I think it has been important to have companies consider moving forward in this whole process, companies that are working nationally, often globally. I think that it has been very, very important for them to say, okay, if we are going to buy off on reasonable access, if we are going to buy off on some of the other things, then we really think one standard nationwide is the way to go, and without that, it is very hard for the companies to explain to themselves sort of what is achieved for simplicity out of the process.

So that is the explanation for the scope of the bill, anyway, you would expect Federal preemption and expect to have some new consumer guarantees such as access with that.

MS. SCHAKOWSKY. It is heartening that some of the major corporations at the very highest level have bought into this process, into this notion.

Dr. Lenard, this committee has been dealing a lot with identity theft, with the problem of personal consumer information. Quite frankly, I have never really heard someone come before us and make the argument that this really isn't a very serious problem.

We are hearing that identity theft is the fastest growing problem. We are constantly barraged with horror stories of people whose lives have been complicated if not ruined by the notion of identity theft. So why is it that you think that it is not particularly a big deal for us to be worrying about?

DR. LENARD. Well, a couple of things. First of all, I think there are two separate issues: One is the legal use of personal information in business, in commerce. Obviously, identity theft is illegal. A good deal of what I was trying to say is that I don't think there is evidence of a market failure or consumer harm from the legal and legitimate use of personal information in commerce. I don't think there is evidence of it. Obviously, they are closely related. Identity theft is not, according to the data, a growing problem. The costs of identity theft have been relatively constant over the last 3 years, which suggests that they have been shrinking in a growing economy; they are shrinking relative to the amount of--

MS. SCHAKOWSKY. Can I interrupt for one second? I would be curious about where you get your data because the FTC has told us that this problem is in fact increasing.

DR. LENARD. It is a report by Javelin, which I would be happy to provide.

MS. SCHAKOWSKY. That would be great. Thank you. Go ahead. I interrupted you.

DR. LENARD. And the Javelin report suggests that actually the number of people subject to identity fraud has declined by 12 percent over the last couple of years. There is a lot of data showing that the losses due to fraud, credit cards, per $100 are at the lowest level. They have declined substantially over the last several years. It is not surprising because most of these costs are borne by the businesses so they have incentive to make the investments in security to try to reduce those costs.

MS. SCHAKOWSKY. The FTC has said that the cost is about--this fraud is about $50 billion a year. I understand that you are saying that business itself has an incentive since they bear most of the cost, but I would be interested in the source of the data that you have just presented.

Mr. Taylor, you are a CPO. Is that a common position in large corporations now?

MR. TAYLOR. Yes, I think it is a common position. It is growing over time. We have seen a lot of growth in the chief privacy officer positions in companies, especially in the last 3 to 5 years. It is a position that is put in place to ensure that as we look at some of the emerging legislation, rules around the world, that we have somebody in place to actually interpret those for the company, working with legal and other organizations, and ensure that we are deploying a policy that is going to protect customers and consumers' personally-identifiable information.

MS. SCHAKOWSKY. Professor Swire, since you fulfilled that role essentially for the Federal government, are you saying we don't have that position any longer and do you think that that would be valuable to have a privacy czar for the Federal government?

MR. SWIRE. It was done exclusively the first time. It is a little bit hard to answer in some ways except that the decision was made when the current Administration came in not to fill that role. I think so many things in the Federal government go across agencies that it makes sense to have someone looking at privacy across agencies and so having somebody in the executive office of the President, I think, does make sense.

MS. SCHAKOWSKY. Certainly seems that way to me, given the use of private information that we are increasingly finding out about, some

legal, maybe not legal in some cases, that we have someone whose job it is to focus on that.

I am out of time. Thank you.

MR. STEARNS. The gentleman from Texas, the Full Committee Chairman is recognized.

CHAIRMAN BARTON. Thank you, Mr. Chairman.

I just want a show of hands on this. How many of the witnesses today support a Federal preemptive privacy standard? Three. Reluctant, four. So we are on record on that.

Would a Federal standard preempt a State from adopting a stricter standard?

MR. SWIRE. I think that is what we have been understanding by preemption. Uniform, yes.

CHAIRMAN BARTON. Uniform standards, and that would preempt States from obviously weakening it but obviously strengthening it.

On the private right of action, the gentlelady from eBay does not support that; isn't that correct?

MS. WHITMAN. Correct.

CHAIRMAN BARTON. Would you support a limited private right of action where you would limit the award to reasonable attorney's fees in some specific capped dollar amount, $250,000 or something like that, as opposed to an unlimited private right of action?

MS. WHITMAN. Let me consult my chief privacy officer.

I would love to kind of think about this a little more. I will give you a tentative answer that I think we would like to have one enforcement agency--that would be the FTC--that would be sort of held accountable. Again, what I am trying to do is simplify our lives, our users' lives and at the same time very robustly supporting a Federal privacy legislation. So let's take that under advisement, and we can get back to you.

CHAIRMAN BARTON. I am not for unlimited private right of action, but I can see when somebody abuses my privacy, I can see wanting to take a private right of action that redresses that specific crime and gives me some financial reimbursement. So that is just an option of going one way or the other.

MS. WHITMAN. Let us think about that a little bit, and we can get back to you.

CHAIRMAN BARTON. Professor Taylor, you speak on behalf of 12 companies. Can you read those companies into the record, please?

MR. SWIRE. I think that was directed to me. Twelve companies--

CHAIRMAN BARTON. I'm sorry. There are five name tags and only four people. So two of you represent two people.

MR. SWIRE. Alphabetically listed, Eastman Kodak; eBay; Inc.; Eli Lilly and Company; Google, Inc.; Hewitt and Associates;

Hewlett-Packard Company; Intel Corp.; Microsoft Corp.; Oracle Corporation; Procter & Gamble Company; Sun Microsystems, Inc.; and Symantec Corporation.

CHAIRMAN BARTON. Do you happen to know where a company like AOL might be in this issue?

MR. SWIRE. We have talked to quite a few different companies. To my recollection, we haven't had a meeting with AOL so I don't have information on that.

CHAIRMAN BARTON. Dr. Lenard, you seem to be the one that seems to indicate there is not a real problem here. Do you not read the newspapers, watch television? Do you not see all of these data security breaches? Citigroup is even running commercials on TV about identity theft. How can you honestly sit here and tell this committee this is not a growing problem?

DR. LENARD. Well, I guess there are a couple of things; One is, I think privacy--obviously they are interrelated--but privacy and identity theft, I am not sure--most of what is talked about in terms of privacy legislation I am not sure would have much--it is not obvious to me the connection between that and identity theft, but I think there is a lot more of kind of hue and cry. As I strive to say in my testimony, I think the facts are actually contrary to the public perception in a number of regards and, then when you look at the facts closely, that the market is working pretty well. It is obviously a rapidly changing technological environment. There is not, as far as I can see, consumer harm from legitimate commercial use of personal information, legal commercial use of personal information. Obviously, identity theft and identity fraud are illegal, and obviously, we need enforcement against it.

But the fact is that there are incentives at work in the marketplace, pretty strong incentives to reduce that.

CHAIRMAN BARTON. Are you familiar with the term pretexting?

DR. LENARD. Yes, I am familiar with it. I am not saying--

CHAIRMAN BARTON. There are companies now in existence to proactively invade your privacy and sell the results of their ill-gotten gains to anybody with a hundred bucks. And we have a bill that has passed this committee, hasn't gone to the floor yet, but you don't consider that to be a problem?

DR. LENARD. Obviously, it is.

CHAIRMAN BARTON. The concept of spoofing, where people send false ID information on your telephone caller ID. I can go on and on and on.

DR. LENARD. Obviously, those are bad things, and that is a legitimate law enforcement problem.

CHAIRMAN BARTON. You did hold you your hand up that you support a comprehensive Federal privacy--

DR. LENARD. I support--I think the major rationale for privacy legislation is Federal preemption, in other words, I think--

CHAIRMAN BARTON. To the extent it is a problem, you think we need a Federal standard on it.

DR. LENARD. To the extent we have a lot of different State laws and inconsistent State laws that people in companies have to deal with, it is better to have one Federal law.

CHAIRMAN BARTON. Mr. Chairman, my time has expired.

MR. STEARNS. I thank the gentleman.

Ms. Whitman has left, and I understand that Scott Shipman, the Chief Privacy Officer, is standing in.

CHAIRMAN BARTON. What happened to Mr. Hendricks?

MR. STEARNS. He said he had to catch a train. I gave him an opportunity to answer about his opening statement, and he decided he had to leave.

The gentlelady from Tennessee, Mrs. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman.

Let's see where I want to start here. Let's go back. In the opening statement, I said something about the EU standards. Professor Swire, I think I will come to you with this one. When you look at the standards that are used there, we continue to hear this a good bit. Is that something you would default to more or less?

MR. SWIRE. Accepting a European approach? Is that the question?

MRS. BLACKBURN. Basically. Are theirs tighter than ours? Are they doing a better job than our private companies are doing here?

MR. SWIRE. Well, I actually wrote a book on that back in 1998 which probably three people made it through without their eyes glazing over, but I think that--

MRS. BLACKBURN. You are saying you are ahead of your time.

MR. SWIRE. Could be. The European rules are not business friendly in important respects, in ways that don't help consumers but put a lot of burdens on businesses.

MRS. BLACKBURN. That is helpful to know, and I appreciate that.

All right. Let's see, I think it is Mr. Taylor. I have got so many sheets of paper with me right now. Your company's policies, do you have the same policy globally, or do these change from market to market when you are looking at privacy policy?

MR. TAYLOR. Our master privacy policy is consistent globally. Same principles apply in all cases. There are some minute changes that are necessary in certain countries, but the base policy is the same everywhere in the world.

MRS. BLACKBURN. Okay. Well, Professor Swire, let me come back to you. If we were to write a comprehensive bill, what are maybe the top components of that that you think we should include?

MR. SWIRE. Well, in our statement, we took a list; that is the list that the Federal Trade Commission has often used. There should be notice to individuals. There should be choice. We say there should be reasonable access, which is something that has been controversial sometimes. There needs to be data security. There needs to be accountability.

MRS. BLACKBURN. You are saying, keep it very simple and broad.

MR. SWIRE. I think so. You have a big country here with a lot of different industries, and if you write a statute that tries to lock in how some people do it, other people do it a different way, so you have to be cautious about that.

MRS. BLACKBURN. And the industry is still changing, and it is new, and it is young.

Dr. Lenard, you mention a Javelin Strategy & Research report that must be just absolutely amazing. I am kind of from the same school of thought as the Chairman, I find it incredible that, in your statement, you say, since 2003, the number of victims has declined by almost 12 percent to 8.9 million annually while the average cost per victim has increased over 20 percent.

My goodness, to me that is just an astounding statistic that the level of individual fraud and the crime perpetrated on the holder of the information, the owner of that information by someone who has created that theft. And then you go on with your explanation: However, since most victims don't incur the costs related to their fraud cases, the average consumer costs have declined by 24 percent, although the time it takes to resolve the fraud case has increased from 33 to 40 hours.

To me that is just astounding that it takes that much time. And when we hold identity theft town hall meetings and we hear from individuals, they are horrified with what has happened to them and the amount of time. I think 40 hours is, from some of the stories I have heard, if people got through that in that period of time, they would consider themselves very fortunate, because for some people, it takes months and months and month to unravel this once their information has been listed.

So if you will please submit a copy of that study and that report, I would appreciate being able to see that and read through that. It would be helpful.

My last question, Mr. Shipman, payment systems, such as Paypal, do you want to give a very brief step of the--when I go on eBay and make a purchase and I submit my information to Paypal, and then they give me my receipt number; then why don't you walk through that process, the steps that are taken for protecting that personal information? How do I

have confidence that that transaction really has completed itself and completed itself in privacy, which sometimes you sit there and you say, well, I haven't seen my goods yet; I haven't seen the things I purchased yet, and oh, my goodness, I hope it went to the right spot.

Why don't you walk us through that?

MR. SHIPMAN. Certainly. Thank you. I think that the key step to note with Paypal is that, unlike purchasing at a restaurant or purchasing in a store, the seller actually does not ever receive the purchase instrument that you have used to provide that payment. That is where Paypal--

MRS. BLACKBURN. The purchase instrument?

MR. SHIPMAN. The credit card, check, bank account number. That is where Paypal in and of itself is a privately enabled--

MRS. BLACKBURN. Let's back up. So the actual merchant never gets that? That just goes to Paypal? So you have taken one person--you are not a three-party transaction, you are simply a two-party.

MR. SHIPMAN. So what in effect happens is the seller is paid without ever seeing your credit card number, your checking account, your bank account, and therefore, they don't have the opportunity, one, to do something wrong if they intended to; and two, to lose it if they didn't intend to do anything wrong but otherwise would care less. In and of itself, there is a privacy system built in.

MRS. BLACKBURN. Very good. Thank you. I yield back.

MR. STEARNS. I thank the gentlelady.

Mr. Gonzalez of Texas.

MR. GONZALEZ. Thank you very much. I got an e-mail a minute ago, one of my staff members who knew about our hearing today, he said: Ironically, some scam artist sent out a mass e-mail this morning using eBay as a cover to find personal information.

So it is happening as we speak, and that is just the price we pay for technology. All the advantages it gives us, obviously, there is exposure.

Professor Swire, if you would help me think this through. If we didn't have any State regulation regarding privacy duties and responsibilities on the part of the companies and we didn't have any Federal statute, Gramm-Leach-Bliley, just doesn't matter, what would be the basis for those companies as far as any liabilities, responsibilities or duties?

MR. SWIRE. Part of it would come from State common law. Is there any tort that happened here? Is there some contract that got broken? And the contracts that get broken, the Federal Trade Commission might come in and say, you did something deceptive. So the base line has been, if a company promises to take care of your information and breaks the promise, that is a deceptive trade practice. And so the FTC or the

State AGs have been able to bring actions when those things happen. It is State enforcement, but it is enforcing the broken promise, broken contract.

MR. GONZALEZ. What about the individual consumer?

MR. SWIRE. Common law has not done very well here at all. Basically, when it comes to information privacy, common law has not developed, and there is, with rare exceptions, no common law way to proceed.

MR. GONZALEZ. So, but for some sort of State or Federal regulatory scheme that would empower a consumer to bring a cause of action, we probably don't have anything out there.

MR. SWIRE. With rare exceptions, yes.

MR. GONZALEZ. What we may have out there right now under the discussion we are having here, and if we had Ms. Whitman and Mr. Taylor's way, we would not have that individual or consumer right cause of action.

MR. SWIRE. That is one of the arguments. Do you have private right? Do you have State AGs, FTC; who gets to be involved?

MR. GONZALEZ. Do you see an advantage to having a private cause of action right?

MR. SWIRE. Today I am here trying to speak on behalf of this Forum of people with different perspectives on this and some other issues, and we hope to have a principles document that comes out with more detail later, but we are not quite there yet today.

MR. GONZALEZ. Wouldn't you say the objective of most laws is to make a person whole again? The individual that is harmed, the individual that suffers the loss.

MR. SWIRE. When I teach torts, that is what you say; we are supposed to get you back to where you started.

MR. GONZALEZ. But this would be an exception to that because if it was Charlie Gonzalez's information that is mishandled, misused, and so on, I don't have a cause of action. It is only if some elected official or appointed official in the State or Federal government chooses to prosecute, chooses to bring a cause of action.

MR. SWIRE. That is the logic for private rights of action when you have torts as the basic way to proceed; that is the reason.

MR. GONZALEZ. I wouldn't have that. The only remedy that we are seeking here, if we are talking about preemption at the Federal level without a private cause of action in any form, shape, or manner, and not even what the Chairman of the Full Committee is suggesting, Charlie Gonzalez is never going to be made whole again. Whatever I lost, whatever my identity theft resulted in my economic loss, reputation, and so on, I would have no cause of action. I would just suffer that loss.

MR. SWIRE. You are making the argument for a private right of action.

MR. GONZALEZ. I definitely know that is what I am doing, because that is my reference, to be honest with you. When we talk about Federal anything and about preemption, it seems to me that we have--and I am not doing a number on corporate America or business mindsets or anything like that. I understand how it works. But it seems to me that they always come to us and say, we shouldn't have a private cause of action, there will be lawsuit abuse. We will have the class actions and such, even though we have some Federal law regarding class actions now, as I understand it is.

But I really do believe we are taking away a valuable right, and that right belongs to the individual consumer that trusted the individual that they shared that information with to keep their promise about safeguarding that information without any kind of negligence or any kind of ill will or intentional tort. I don't understand why we actually do that.

So let me ask, and I know Ms. Whitman is gone. Is it Mr. Shipman?

MR. SHIPMAN. Shipman.

MR. GONZALEZ. What is your position? Why would you all fear your individual customer to come to you and say, hey, you breached your agreement with me; you said you would safeguard my information, and you didn't? What is so wrong with that individual having some sort of remedy to seeking some redress?

MR. SHIPMAN. I think it is entirely appropriate for an individual at some level to have a remedy, and certainly what was said earlier was that there is a balance that needs to take place. There is certainly a concern that we don't want to overburden business. We don't want to overburden eBay's sellers that run business. We don't want to overburden the myriad of hundreds of thousands of eBay sellers that run small businesses.

With that said, I think to the extent that what I have heard of the conversation today talking about is we want to provide some sort of remedy, and certainly, if we look to the examples of either CAN-SPAM or some of the other laws that Professor Peter Swire has mentioned, I think we do see there are examples that have worked where it is a large, broad uniform Federal legislation that has a strong preemptive component but then may allow AG enforcement to provide the customer or the consumer with a level of individual protection, individual right.

Certainly, we are not there yet, and what we are talking about is a discussion on Federal privacy legislation and where we are at in that principles document is certainly evolving. But, naturally, it does beg the question to look and see what has worked and what is out there working, and actually, I think that would be a good place to start.

MR. GONZALEZ. The beauty of a private cause of action, it belongs to the individual citizen, and it doesn't necessarily have to depend on the whims or political considerations of an elected official or an appointed official because I will tell you right now that goes into the mix of factors in deciding whether there is going to be enforcement of any particular regulatory statute out there, whether it is State or Federal level. I have seen it. I have experienced it. Everybody is guilty of it, regardless, at some point in time politically, and it is just wrong. I am hoping that we again maybe seek that balance that Ms. Whitman was talking about. Again, I am going to Dr. Lenard's concern not to have a regulatory scheme that makes the legal collection, dissemination and sharing of information so difficult that it bogs down our economic system and actually can be a deterrence or impediment to technological advances in a healthy marketplace.

With that, I yield back the balance of my time.

MR. STEARNS. Mr. Deal, the gentleman from Georgia.

MR. DEAL. I thank you.

Last week this Full Committee passed a health information technology bill. We did not include in that privacy language. There are those who wanted us to do so; others who said that it is not the appropriate vehicle for doing it.

My first question is: Is the health information arena so different that it cannot be adequately encompassed within some overarching uniform privacy standards, and if it is not, why not?

MR. SWIRE. I think, from the panel, I spent the most time living through HIPAA and all its wonders. A couple of observations: One thing is that, for the over one million covered entities who are under HIPAA today, they have gone through a big process already that other sectors haven't gone through in quite the same way, so they have gone and bought systems and put in security and privacy. And so when I talk to health care people, they think the idea of tearing that down and having to do something different is unfair to them. That is one observation about health IT.

Another thing is that there is a series of public concerns around health care information that are pretty special. Health care research is a very special universe. How are you going to do the medical research to save all our lives or our grandchildren's lives? So there are some very special things in health care that are pretty different as a sector. So those are two reasons for caution in saying, heck, let's just put it all off into a different thing. I think the third and final point is health care is inside your body, inside your brain. It is very sensitive data and people sort of think of that as way up there on the sensitive scale.

MR. DEAL. So rather than having to undue HIPAA, perhaps we should look at refining additional privacy rules, if necessary, to deal with the implementation and encouraging the implementation of health records being computerized, et cetera, and interoperability among hospitals, doctors offices, and other medical providers. Is that generally what I hear you saying?

MR. SWIRE. Let me be really, really clear, this is individually me speaking here, this is not the forum.

MR. DEAL. I have the rare opportunity on behalf of all the law students in the country to cross-examine a tort professor, something I have always wanted to do.

MR. SWIRE. I have a few students in the room here today who are enjoying it.

The question is, to refine the health care but not try to merge them, and I think that is the direction that I would be pointing to.

MR. DEAL. All right. Let me go to a broader issue here, and that relates to rights of actions and the basis for rights of action. It seems to me that there are some very different issues, and I think Dr. Lenard tried to distinguish between the identity theft issue and privacy breaches. They may not necessarily be the same. They may be the same, but they may not necessarily be the same.

With regard to that, is it possible to devise a regulatory, or a statutory rather, format that defines the responsibility of information collection systems, whether it be, in the commercial sector, and define those responsibilities? And if a company conforms to those requirements, that they would not be liable in an action either administratively or a private right of action for individuals, for example, who are able to breach that system or for individuals within their own corporate structure who certainly without authority breach the system and use information outside?

I am not sure that I am communicating my concerns. My concern is, are we able to define a standard of care statutorily that a corporation or a business can say we have complied with this, but nevertheless, there may be identity theft; there may be breaches that perhaps they were unable to prevent. Is that a realistic goal? Because I don't think we can ever hold people to an absolute standard. In other words, is it going to be a strict liability standard? Is that what is being asked, strict liability?

MR. SWIRE. It sounded for a moment as though you were saying, could there be a safe harbor area?

MR. DEAL. Let me put it in another situation, in a medical context. If we are dealing with medical malpractice, there are standards of conduct that are the test by which the determination is made whether or not there is negligence that leads to a cause of action. That is the same

kind of analogy I would make here. Or are we going to have a standard that is a strict liability standard without regard for due diligence, without regard to lack of negligence? What are we talking about?

MR. SWIRE. This is one place where this is in more detail than at least the Forum as a group has gotten to something yet.

MR. DEAL. Don't you think that is where the heart of this issue might lie?

MR. SWIRE. In every regulatory regime, you have mens rea issues. What is intentional enough to get you extra bad or is negligent, or is it going to be strict liability? So that is something that has to be very clear or else people don't know what game they are playing.

MR. SHIPMAN. I think that what we are seeing from the FTC today is certainly a security standard through their enforcement actions. If you read the various documents that they publish and review the cases, out of that is evolving a standard. Now I think to your question, can you draw a line and say, to the left of that is one thing and to the right of that is another, and the challenge there is naturally technology, and technology, as we all know, continues to move.

So to create any type of strict standard where you follow that line could be problematic on both fronts. One, it could become too weak of a standard at some point, or it could be too strict based on where we draw it.

MR. DEAL. Mr. Chairman, with your indulgence Mr. Terry had to leave and if I may ask a question on his behalf. Since we are talking about the possibility of preempting State statutes, his question was, is there any State that the panel is aware of that has done a very thorough job of adopting State protections by State statute? And if so, who are they? Are there some models out there at the State level that you would recommend?

MR. SWIRE. Perhaps not surprisingly, California has been active in the area and has been more regulatory than most States. For certain financial records, Vermont has been more regulatory than more States; North Dakota at one point. So there is a fair bit of variation out there. I don't have one State to hold up as the perfect one for there has been a fair bit of experimentation.

MR. DEAL. Thank you.

MR. STEARNS. Thank you. Mr. Otter has left so I think we have concluded. I would just ask Mr. Lenard, isn't it true that, in the European Union, they had no private right of action in their privacy legislation?

Mr. Shipman, isn't that true?

MR. SHIPMAN. That is correct, based on my understanding.

MR. STEARNS. Mr. Taylor.

MR. TAYLOR. Yes.

MR. STEARNS. So over in the European Union, they are pretty much highly regulatory, and yet they have no private right of action. And in fact, you have to pay your own attorney's fees.

I guess the one question I have before we conclude is, we put together a bill here and then you do business in the European Union, how does the handling of business in countries that have different regulatory schemes, how does that affect eBay, if someone works for Hewlett-Packard--how does eBay handle somebody in the European Union with a different set of privacy regulations if we passed a Federal bill?

MR. SHIPMAN. That is a challenge for large sellers as well as for eBay, Paypal, and Skype. One of the things we have worked very hard on is synchronizing our own policies and access, as we talked about earlier, to make sure all of our customers have a baseline standard with which they can expect to receive information, answer questions, and access their information across the eBay platform.

So the simplest form of answer to you is that providing Federal legislation in the United States actually makes it easier, because in fact we now have a standard to point to within the U.S. as we already do within Europe and certainly within the APEC framework in Asia.

MR. STEARNS. Anyone else like to comment before we conclude?

MR. TAYLOR. I would be happy to comment.

Very similar scenario at HP. When the European Union established safe harbor and developed principles, HP actually built its privacy principles in our policy against the EU standard, and we did that really for the simple purpose of being able to have one consistent global standard that met the requirements or the bar every place in the world.

MR. STEARNS. Wouldn't that be another reason why we as Members of Congress when we legislate here should take into account some of the other continents' privacy to try to at least as much as possible have one regulatory scheme that would be universal application so companies like you can do international global business without fear of different kinds of litigation problems or standards?

MR. TAYLOR. HP certainly isn't advocating adopting the EU standard, but I think, as we develop the framework and look at the principles, I think it is important for us to look at other best practices and what other countries or groups of countries have done. I think there are things that we can do.

MR. STEARNS. Mr. Shipman, would you like to see the United States adopt the European standard?

MR. SHIPMAN. Absolutely not. This is America, and I think, as such, I think we need laws that make sense for us. Certainly, we do have

the luxury of time, which is we can see what has worked and what hasn't worked.

MR. STEARNS. In the European Union standard.

Dr. Lenard.

DR. LENARD. The one thing I would add is that, in the APEC, the APEC framework as distinct from the European framework has harm as a central feature of it, so that the regulation--that is obviously a big advantage. I think that is something to look to for some guidance.

MR. STEARNS. Professor Swire, anything you want to comment?

If not, I want to thank all of you for your patience, and I think we had a very balanced hearing, and I appreciate your attention. And with that, the subcommittee is adjourned.

[Whereupon, at 4:14 p.m., the subcommittee was adjourned.]

○